602LAN SUITE 2004
User Manual

Table of Contents

Introduction to 602LAN SUITE 2004 3
What is 602LAN SUITE? 3
Installation 6

Basic Setup 7
Setting Up Your Internet Connection 7
Setting Up User Accounts 9
Configuring Your E-mail Server 12
Configuring Your Anti-virus Protection 16
Configuring E-mail Client Access 17
Configuring Your Web Server 18
Configuring Your Fax Server 22
Configuring Shared Internet Access 26

Basic Administration 28
Administration Configuration 28
Administration via the Application 28
Web Based Administration 28
Logging Server Activity 31
Installing as a Windows Service 33
DHCP Server Setup 34

Advanced Features 35
SMTP Authentication & Settings 35
Web Mail 37
WAP Access 44
Anti-Spam Protection 45
LDAP Address Book Setup 49
Attachment Filter 50
Update Manager 51
ActiveReports 52

Advanced Access Control 55
Firewall 55
Proxy 59
Proxy Cache 61
Site Access Control 62
Mapped Links 63
Proxy IP Filter Configuration 65
SSL Configuration 68

Appendix 70
Hayes Compatible Modem Commands 70
E-mail Settings Example 72
Troubleshooting Common Error Messages 73

© 2004 Software602, Inc. 9/2004

Introduction to 602LAN SUITE 2004

What is 602LAN SUITE?

602LAN SUITE is a secure mail server with anti-virus & anti-spam, built-in firewall with NAT and proxy for controlled Internet sharing! This all-in-one server application is completely FREE for 5 users and additional user licenses are available for purchase at http://www.software602.com/store/. 602LAN SUITE is developed exclusively for the 32-bit Windows 98/ME/NT/2000/XP/2003 environment. Some features may not be available in the Windows 98/ME environment. You may download the most current version of 602LAN SUITE at http://www.software602.com/download/.

General Features

- SMTP and SSL SMTP server
- POP3 and SSL POP3 server
- Web Mail Client
- Fax server through a TAPI device (fax modem)
- Firewall
- NAT (Network Address Translation)
- Functions as a SOCKS proxy
- Provides a PROXY for HTTP/HTTPS/HTTP-FTP, FTP, SOCKS, Telnet and RealAudio with cache
- Works as an IP Filter
- Web and SSL Web server with ISAPI, CGI and FastCGI access
- DHCP Server
- LDAP Address Book
- Anti-virus Protection
- Anti-spam Protection
- Attachment Filter
- Update Manager
- ActiveReports Plug-in

Feature Descriptions

SMTP Server

One of the main functions of the server is to provide direct sending and receiving of Internet messages by the SMTP (Simple Mail Transfer Protocol) protocol. Direct transmission between 602LAN SUITE and the Internet can occur without the need for any e-mail provider service. Using this method the server will deliver the e-mail directly to the user's mailbox from the Internet, and it "listens" on the port that is allocated for the SMTP protocol (default 25). If message packets begin to arrive, the server provides further processing. You also have the option of setting up SSL security on the SMTP server to ensure secure communication between the server and the client.

POP3 Server

602LAN SUITE works as a POP3 (Post Office Protocol v.3) server and also as a SSL POP3 server to provide access to the messages located in the user's mailbox from any client program which supports the POP3 protocol (Microsoft Exchange, Outlook Express, Netscape Messenger, Eudora, etc.). You also have the option of setting up SSL security on the POP3 server to ensure secure communication between the server and the client.

Web Mail Client

The Web Mail Client provides access to 602LAN SUITE mailboxes through a browser. All communication between the browser (client) and 602LAN SUITE (server) is running through the HTTP or HTTPS (Secure HTTP) protocol.

Fax Server
The Fax Server works through a TAPI device (fax modem). If you check Fax server on the Fax/General tab, all faxes will be sent and received through the TAPI device. Incoming faxes will be routed to a user's mailbox according to the Fax IDs entered on the Users/Properties tab or to a user with the Route unsorted faxes/messages to this user right (check the Users/Properties tab).

Firewall
The firewall protects the computer where 602LAN SUITE is running and the entire Local Area Network against unauthorized TCP/IP connections. 602LAN SUITE's firewall is based on rules composed into sets. If no rules are entered, all TCP/IP connections are prohibited.

NAT
NAT stands for Network Address Translation. The idea behind NAT is to re-write the IP headers and substitute one numeric address for another. Network Address Translation allows a single device, such as the computer where 602LAN SUITE is installed, to act as a gateway between the Internet (or public network) and a local (or private) network. This means that only a single IP address is required to serve a group of computers.

SOCKS
Originally, SOCKS was developed by David Koblas and later was modified and extended into its present version – version 5. It is a protocol that switches TCP tasks on the computer with the firewall thus enabling the user applications to pass transparently through the firewall. Because this protocol is independent of the application protocols, it is used for many services, such as telnet, ftp, gopher, WWW, etc. The server transmits data between the client and the application server with minimum load on the processor. Because SOCKS does not work with application protocols, it can be easily used with protocols that implement encryption to provide protection during transmission.

Proxy
The proxy brings an advantage that only one IP address from the provider is needed to connect the network to the Internet and no router is necessary. The proxy includes cache functions for the particular protocol. The proxy always operates on a particular communication protocol. The client program must support communication through a proxy. 602LAN SUITE's Proxy supports HTTP/HTTPS/HTTP-FTP, FTP, SOCKS, Telnet, RealAudio and HTTP caching. 602LAN SUITE supports a secondary parent proxy or cache server. This second-stage means that 602LAN SUITE will receive data via another proxy/cache server, which for example can be located on the ISP's server.

IP Filter
The IP filter checks the TCP/IP packets according to the IP address, and decides if they are to be denied or granted access to a particular service.

SSL (Secure Socket Layer)
The TCP/IP protocol transports and routes data over the Internet. Other protocols, such as the HyperText Transport Protocol (HTTP), Lightweight Directory Access Protocol (LDAP), or Simple Mail Transfer Protocol (SMTP) run "on top of" TCP/IP in the sense that they all use TCP/IP to support typical application tasks such as displaying web pages or running e-mail servers. SSL runs above TCP/IP and below application level protocols such as HTTP or SMTP. It uses TCP/IP on behalf of the higher-level protocols and in the process allows an SSL-enabled server to authenticate itself to an SSL-enabled client.

WWW Server
The WWW (World Wide Web) and SSL WWW Server provides the presentation of HTML pages that are stored in a specific directory (see WWW tab / Home directory of WWW Server). The WWW Server also provides the ability to create private personal HTML pages for 602LAN SUITE users

DHCP Server
DHCP (Dynamic Host Configuration Protocol) Server gives 602LAN SUITE the ability to dynamically assign IP addresses and other TCP/IP parameters to the client PCs upon request. DHCP parameters can be assigned by the administrator through 602LAN SUITE's Advanced Configuration. DHCP is especially useful when managing large networks.

LDAP Address Book
LDAP (Lightweight Directory Access Protocol) is a standard client-server access protocol to view information in LDAP servers. LDAP's directory service is a powerful search tool that you can use to find people and businesses around the world. 602LAN SUITE includes an LDAP Server that is designed to provide user information. If a specific address needs to be included in the LDAP Address Book, check the Include in list for LDAP Address Book checkbox on the User's properties tab. Each e-mail client that includes an LDAP Client (i.e. Outlook Express) can pick up all e-mail addresses that are provided by the LDAP Address Book.

Anti-virus Protection
602LAN SUITE Anti-virus Edition provides scanning of all messages for viruses using BitDefender Anti-virus technology. All e-mail messages and attachments will be scanned for malicious viruses and worms at the server before they reach your user's mailbox. The BitDefender engine is certified by ICSA Labs.

Anti-spam Protection
Anti-spam protection is used to prevent unsolicited e-mail from entering your network. 602LAN SUITE provides four methods of Anti-spam protection. The first method is via a Bayesian filter, the second by DNS Blacklists (DNS-BL), the third via a server based Blacklist and Whitelist and the fourth is through user based Blacklists and Whitelists.

Attachment Filter
The attachment filter can check messages with attached files by specific extensions and either reject the message or remove the attachment.

Update Manager
602LAN SUITE provides automatic updates. It is possible to set the update check interval and notify the administrator when an update is available.

ActiveReports Plug-in
ActiveReports provides detailed analysis of 602LAN SUITE usage. It simplifies employee activity monitoring to control bandwidth usage and employee time. Easily identify the most visited web sites, sources of junk e-mail, viruses and more. ActiveReports is included with 602LAN SUITE, FREE for 30 days.

Installation

System Requirements

Operating System
Windows 98SE/ME/NT/2000/XP/2003

Memory
Windows 98SE/ME – 32 Megabytes of RAM
Windows NT/2000/XP – 64 Megabytes of RAM
Windows 2003 – 128 Megabytes of RAM

Hard Drive
30 MB for 602LAN SUITE + approx. 10 MB per user mailbox

Additional Notes and Requirements

- You must have a properly operating TCP/IP network in order to use 602LAN SUITE 2004. This means that all clients and servers must be able to properly communicate with one another freely without errors using the TCP/IP protocol prior to the installation of 602LAN SUITE. The server upon which 602LAN SUITE is to be installed must also be connected to and able to browse the Internet.
- Microsoft Internet Explorer 5.0 or later is required to use all features. MSIE 4.0 or later will work for Internet access via the proxy.
- The Windows 98SE/ME operating systems will NOT reliably support over ten users when acting as a network server with 602LAN SUITE. These operating systems are desktop operating systems and were never designed or intended for server applications. Networks consisting of over ten computers are required to use Windows NT/2000/XP/2003 operating systems for 602LAN SUITE.
- The Firewall and NAT functionality is only available on Windows 2000/XP/2003. Computers with multiple processors or processors with Hyper-threading support currently do NOT support the Firewall and NAT functions.
- The Anti-virus Edition provides 1 year of anti-virus updates from the date of registration.

Downloading
You can download 602LAN SUITE from http://www.software602.com/download/ at anytime. When downloading from this location you will always receive the most recent release of 602LAN SUITE.

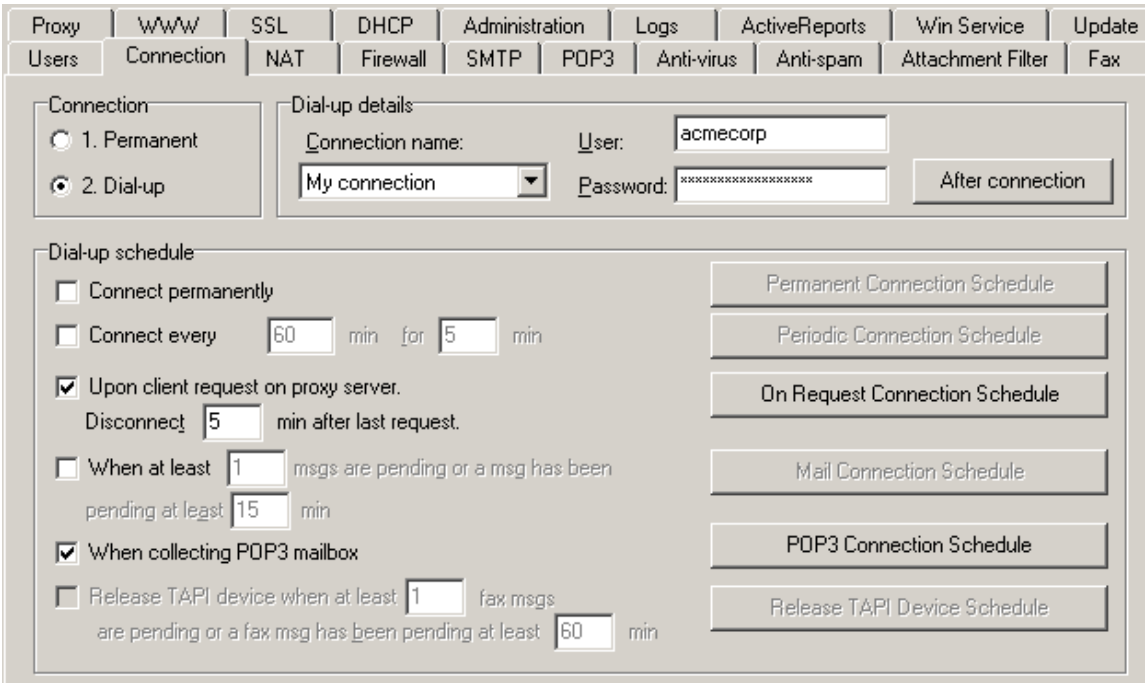
Installing
1. Run ls2004.exe from the directory where you downloaded the program.
2. Follow the directions given by the installation program.
3. After accepting the license agreement, choose a directory where you want to have the program files installed (e.g. C:\Program Files\Software602\602Lan Suite).
4. Choose the name of the folder for the icons. Now all files will be copied to your chosen directory.

602LAN SUITE 2004 installation should now be complete. You must now register the software. For registration assistance, please refer to support site at: http://support.software602.com/

Basic Setup

Setting Up Your Internet Connection

The Connection Tab enables you to specify how you are connected to the Internet. To access the connection setup, open 602LAN SUITE, click on “Settings” then “Advanced Configuration” and finally the “Connection” tab. Basically, there are two options depending on the available connection type.



Permanent Connection

If the connection is made with a permanent line (DSL, Cablemodem, T1, etc.), there is no need to establish a connection. Therefore place the switch to position 1. Permanent. Select this method if you are not connected via a permanent line but there is another computer that provides the connection for you. In fact, this selection means that the program does not care about the connection but only assumes that the connection is established. In such case, all control elements in the tab are grayed and therefore inactive.

Dial-up Connection

If you make a connection via a dial-up line (analog dial-up, ISDN) and you want 602LAN SUITE to establish and terminate the connection, select the option 2. Dial-up and complete the Dial-up schedule (how often you want to establish the connection, etc.). 602LAN SUITE can work with any Windows Dial-up Networking connection.

NOTE: A Dial-up connection MUST be configured in Windows before using 602LAN SUITE!

Dial-up Connection Details

From the list Connection name, select the dial-up profile name you want to use to establish the Internet connection (all information contained in the profile is from your provider, the connection itself is pre-setup in the Windows environment, My Computer / Dial-Up Networking). Fill in the User name and your access Password to the connection. You can obtain this data from your Internet provider.

Secondary connection (VPN)

To configure a secondary connection (VPN connection) click the After connection button. A VPN (Virtual Private Network) is the way to establish a private connection by encoding, authentication or tunneling

through public lines. It is necessary to setup this VPN adapter in Windows 98 or higher (Control Panel / Network – make sure the VPN Adapter is present). Check the After connection button then Establish secondary connection checkbox and select the Connection name, which you have already created in Windows (My Computer / Dial-Up Networking).

The ONCONN.BAT file is used for editing the routing table or to start another batch process. If you need to run a process with the VPN connection, create the file ONCONN.BAT and save it to the folder where 602LAN SUITE is installed and check the Run ONCONN.BAT checkbox.

NOTE: Currently 602LAN SUITE only supports dialing a VPN through a second dial-up modem. PPTP connections via the Internet are not supported.

Establishing a Dial-up Schedule

Upon a Request for Permanent Connection

Check Connect permanently to provide a permanent connection to the Internet. Simultaneously, this activates the button Permanent Connection Schedule. It opens a table that you can use to specify the weekly schedule when the permanent connection is enabled or disabled. This weekly table is divided into half-hour intervals. A green field means that a connection can be established a red field prohibits the connection.

Upon a Request for Periodic Connections

Check Connect every, if you want to connect to the Internet on a regular basis – after a specific time interval. Enter the interval in minutes into the field to the right of the switch and enter the minimum connection time into the next field. The request for a periodic connection activates the button Periodic Connection Schedule, which opens a table to specify the weekly schedule for the connection.

When at least X messages are pending

Check this box when you want 602LAN SUITE to connect to the Internet after X messages having been waiting for X amount of minutes. Use the Mail Connection Schedule button to specify when you want 602LAN SUITE to obey this rule.

When collecting POP3 mailbox

Use this option to tell 602LAN SUITE to connect to the Internet when a POP3 mailbox needs collecting, which is specified on the POP3 tab. Use the POP3 Connection Schedule button to specify when you want 602LAN SUITE to obey this rule.

Upon Client Request on Proxy Server

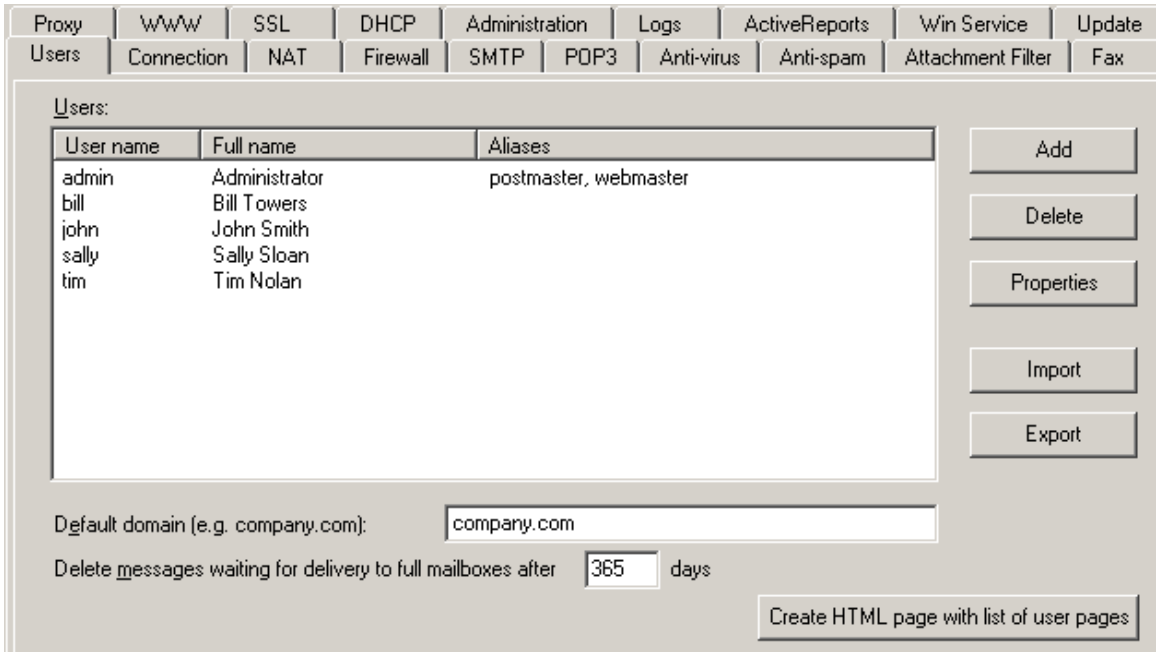
If you want 602LAN SUITE to connect to the Internet upon a client request for SOCKS, DNS or any Proxy services, check Upon client request on proxy server. You must check this if you want the server to connect to the Internet if a client makes a request for the Proxy. Enter the number of minutes into the field Disconnect X min after last request.

Release TAPI Line when at least X Fax messages are pending

This setting allows 602LAN SUITE to share a single dial up modem for both Faxing and Internet/E-mail access. When a specified number of fax messages are waiting to be sent, 602LAN SUITE will automatically release the Internet connection long enough to send the faxes. It will then re-connect to re-establish the connection.

Setting Up User Accounts

The USERS tab can be found by clicking on "Settings" and "Advanced Configuration" from within the 602LAN SUITE 2004 application. User accounts are required for use of 602LAN SUITE's Proxy authentication, Fax and E-mail services. Improper setup of user accounts can result in lost e-mail, denial of e-mail services and even denial of access to the 602LAN SUITE program.



NOTE: Always setup the ADMINISTRATOR account first!

Default Domain

When to use a default domain

You will use a default domain whenever 602LAN SUITE is used as an E-mail server for your registered domain (i.e. mycompany.com). A default domain lets 602LAN SUITE know which Internet domain it is providing e-mail services for.

When not to use a default domain

If you are using 602LAN SUITE for only internal e-mail or if you use only e-mail addresses provided by your local Internet service provider, which end in that providers domain (i.e. @earthlink.net). When this situation occurs, you will need to use aliases as described in the "Creating a user" section.

Delete messages waiting for delivery to full mailboxes after x days

This option is only used if a user mailbox has reached the mailbox limit and e-mail delivered to that mailbox is from POP3 collection and fax messages. If e-mail is sent to a user mailbox that has reached the limit via SMTP the standard SMTP error 450: mailbox full will be returned to the sending SMTP server.

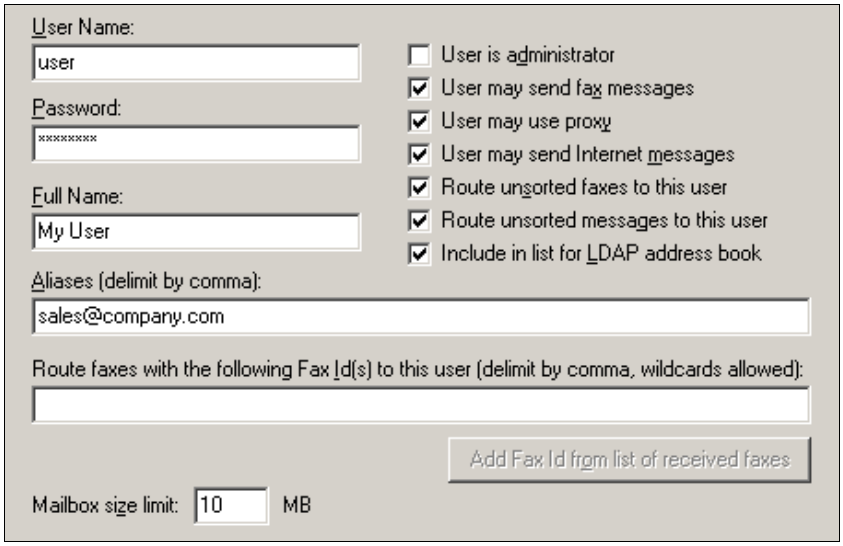
Creating a User

Use the Add button to add a new user account. The add a new user window has six fields and seven checkboxes:

- **User Name** – Enter the user name. The name must be unique (it is checked). This name will be used as the name part of the Internet address. If you entered company.com as the default domain name and bob as the user name, the complete Internet address for this user will be bob@company.com. By default, 602LAN SUITE will only work for clients that are 602LAN SUITE users (see SMTP Authentication

& Settings). Usernames must contain only valid characters. When creating a user name, do not include the @ symbol or the name will be invalid and cause 602LAN SUITE to generate errors when this user attempts to log into to use 602LAN SUITE services.

- **Password** – Enter the password. The password is not case sensitive. The password is written in hidden form (only asterisks are displayed) and characters with diacritics are not allowed.
- **Full Name** – Enter the full name that will be visibly shown in the list for easier user identification.
- **Alias** – If the users e-mail address does not match user@defaultdomain or if the user needs to receive e-mails from multiple e-mail addresses, you must enter an alias for his/her actual e-mail address or the additional e-mail addresses that are intended for the user. An alias is and can only be a complete e-mail address (i.e. someone@mycompany.com). Use a comma or space character as the separator between names.
- **Route faxes with the following Fax Id(s) to this user** – All incoming faxes with the entered Fax Id will be delivered to the mailbox of this user. The Add fax Id from the list of received faxes button opens a window offering a list of received fax Ids. Here it is possible to choose Fax Ids, which will be routed to this user. Use the comma or space character as the separator between Id(s). Wildcard (*) and Mask (?) symbols can be used.
- **Mailbox size limit** – Here you can set the size limit of the user mailbox.



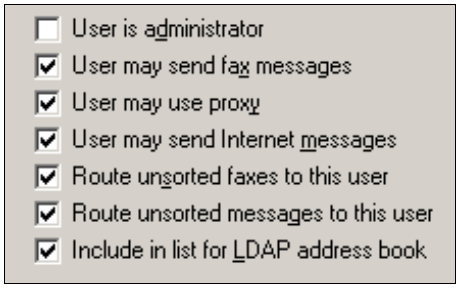
User Rights

When adding a user these check boxes appear to the right of your screen. Check all that should apply to the individual user. **Be sure to create at least one administrator.**

- **User is administrator** – User has the right to administer and remotely administer (via a web browser) 602LAN SUITE.
- **User may send fax messages** – User has the right to send fax messages.
- **User may use proxy** – This rule only works with the Authentication required rule (see Proxy tab). If the Authentication required rule is not checked the User may use proxy rule has no effect. If both rules are checked on, a login window appears when any user attempts to access the **HTTP/HTTPS/HTTP-FTP** proxy. After entering a valid user name and password, the user will have the right to use the proxy[1].
- **User may send Internet messages** – user has the right to send Internet messages. Each 602LAN SUITE user has the right to send local messages but only users granted this rule can send their messages via 602LAN SUITE to the Internet.

[1] This does not effect access to the SOCKS, FTP, Telnet and RealAudio proxies.

- **Route unsorted faxes to this user** – faxes with such Id(s) that do not correspond with any Route faxes with the following Fax Id(s) to this user field will be copied to all users with this right. **NOTE: If at least one user does not have this right, all users will receive unsorted faxes.**
- **Route unsorted messages to this user** – e-mail that has been downloaded via POP3 and cannot be sorted to a user will be copied to all users with this right[2].
- **Include in list for LDAP address book** – if you check this rule, the user will be added to the 602LAN SUITE LDAP address book.

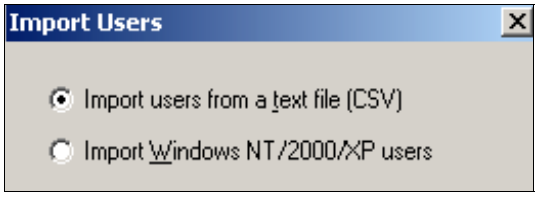

User is administrator
User may send fax messages
User may use proxy
User may send Internet messages
Route unsorted faxes to this user
Route unsorted messages to this user
Include in list for LDAP address book

Aliases
You can use an alias anytime the users e-mail address does not match the User@defaultdomain format or when a user needs to receive multiple e-mail addresses to a single account.

Deleting a User
Use the Delete button to delete a user account. Highlight the user you want to remove, click Delete and the selected user account will be removed.

Import Users
User can be imported from a standard CSV text file or from local Windows NT/2000/XP users.

- **Import users from a text files (CSV)** – Select the CSV file from import, select the fields the import and change assignment as needed, to match the data to import with the correct 602LAN SUITE field.
- **Import Windows NT/2000/XP users** – Select the local Windows users you would like to import, and then click Add selected users.



NOTE: Passwords for imported users can be set one at a time or a default password can be assigned to all users. These users can change their password by using the Web Mail Client.

Export Users
The Export button opens a window offering to save 602LAN SUITE user information (User Name, Full Name, E-mail Address, Aliases, User Rights, Fax Number, Fax Ids and Mailbox Size Limit). You can save the list to a text file with a .TXT or .CSV (Comma Separated Values) extension.

NOTE: The Regional Settings/Number/List Separator value defines the separator.

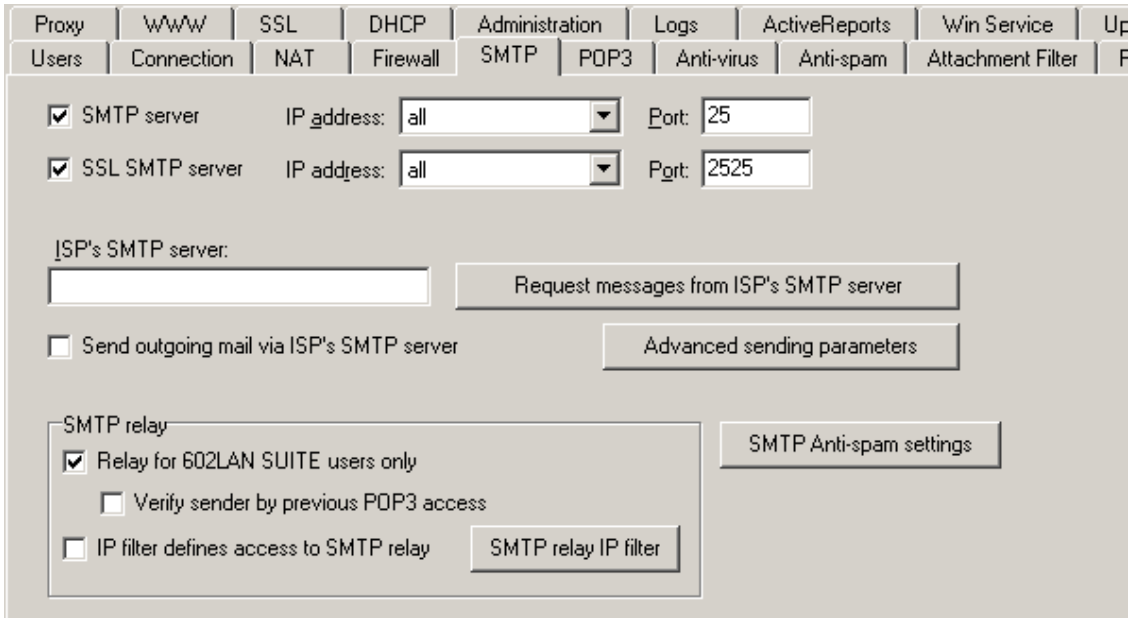
[2] If at least one user does not have this right, all users will receive unsorted messages.

Configuring Your E-mail Server

Basic Configuration

The SMTP tab is used to set parameters that control the transmission of messages via the SMTP protocol. Sending messages out via the SMTP is clear - when a message is waiting and the working intervals are achieved (see Advanced sending parameters), messages are sent out. Receiving messages via the SMTP protocol is different; it requires configuration of 602LAN SUITE and possibly from your Internet/DNS Service Provider.

NOTE: Before configuring the SMTP server for sending or receiving e-mail, be sure you have created all of your user accounts and configured their e-mail address as explained in the "Setting up User Accounts" section of this manual.



SMTP and SSL SMTP Server Settings

It is possible to enable/disable the entire SMTP server by checking on/off the SMTP server checkbox. It is also possible to select the TCP/IP interface where the SMTP server will operate on. All interfaces are selected by default, but you can choose a specific interface from the SMTP server's IP address pull-down box. This allows you to run the SMTP server on only one interface for security or functionality reasons (i.e. setting the SMTP server to the Internal LAN interface will only allow users from the LAN to access the SMTP services). 602LAN SUITE also includes an SSL SMTP server that provides a secure server to client connection. Setup the SSL SMTP server just like the standard SMTP server (above). The default port where the SSL SMTP server listens is 2525. In order to use SSL Security you must first generate an SSL certificate. See the SSL configuration section of this manual for details.

Receiving Messages via the SMTP Protocol

The SMTP protocol assumes that the SMTP server for which messages are delivered to is accessible (i.e. is up and has an established connection to the Internet). If your 602LAN SUITE SMTP server will not be accessible all the time because you use dial-up or some other non-permanent Internet connection, there are two possibilities:

- **Your Internet service provider supports SMTP spooling:** Your ISP's SMTP server sees that your 602LAN SUITE SMTP server is not accessible, it will place messages into your ISP's SMTP spool queue.

- **Your Internet service provider does not support SMTP spooling:** Your ISP's SMTP sees that your 602LAN SUITE SMTP server is not accessible, it will place messages that should be delivered to your 602LAN SUITE SMTP server into a POP3 mailbox that your ISP has created for you.

Selecting the Message Processing Method

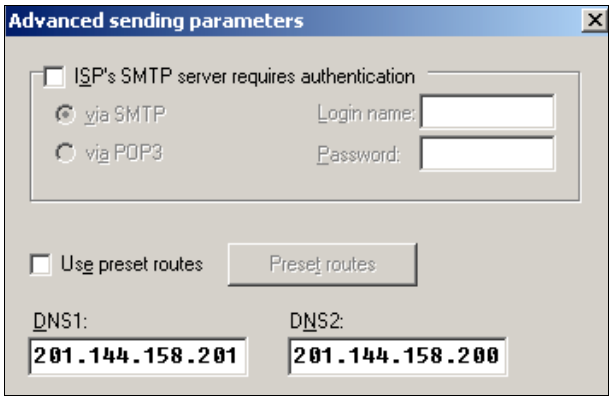
Send Outgoing Messages via ISP's SMTP Server

The simplest situation for delivering e-mail is if you can offload delivery to your Internet Provider's SMTP server. In this case, enter its address, either in the IP or domain form into the field ISP's SMTP server and check Send outgoing mail via ISP's SMTP server checkbox.

NOTE: We recommend using this option of delivering e-mail when using a dial-up connection since the Internet Provider's connection is much faster.

Send Outgoing Messages Directly to the Internet Using DNS

The standard method of routing e-mail uses DNS (Domain Name System) services to request the MX record information about where the e-mail for a particular domain is to be directed. DNS evaluates your request and if it does not find a corresponding MX record, it forwards the request to the nearest DNS. This procedure is repeated until the corresponding record is found and the destination address is found. Uncheck the Send outgoing mail via ISP's SMTP server checkbox, click Advanced sending parameters and enter the IP address of your DNS (this was assigned to you by your Internet Provider) into the field DNS1 and DNS2 (DNS2 is optional).



NOTE: We recommend using this option of delivering e-mail when using a permanent Internet connection.

Request E-mail from the ISP's SMTP Server

If your Internet Service Provider provides e-mail spooling services, it is possible to collect e-mail through the SMTP server even if you do not have a permanent connection to the Internet. Some Internet Service Providers support ETRN or ATRN as an e-mail collection request. If your Internet Service Provider supports SMTP spooling via ETRN or ATRN, click the **Request messages from ISP's SMTP server** button.

ETRN

ETRN (Extended TURN) is an ESMTP command (first defined in RFC 1985) with which a client (602LAN SUITE) using a static IP address asks the server (your ISP's SMTP server) to deliver queued e-mail to the client (602LAN SUITE) via a new ESMTP connection. The parameter is usually the domain name. Please check your ISP for the correct ETRN command format.

ATRN

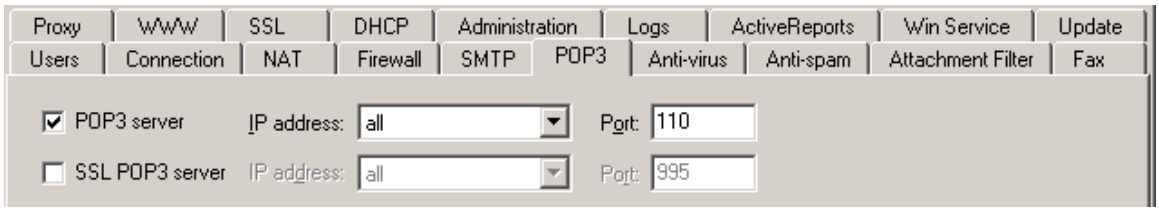
ATRN (Authenticated TURN), also known as On-Demand Mail Relay (ODMR), is an e-mail service that allows a user to connect to an Internet service provider (ISP), authenticate, and request e-mail using a dynamic IP address from any Internet connection. The details about ODMR can be found in RFC 2645. To

use ATRN, check the ATRN switch. ATRN requires authentication on the remote server via a username and password. The parameter is usually the domain name. Please check your ISP for the correct ATRN command format.

Request messages
Here you need to setup when the request for the e-mail will be sent. Check one or both checkboxes: **When a dial-up connection is established** and **Every** x **minutes** checkboxes. According to this setting 602LAN SUITE will send the ETRN or ATRN collection command to the Internet Service Provider and e-mail collection will begin.

POP3 and SSL POP3 Server Settings

Post Office Protocol 3 (POP3) is the name of the protocol used for collecting the contents of mailboxes on the Internet. On the POP3 tab you can specify which POP3 mailboxes you would like 602LAN SUITE to collect and distribute. By simply enabling the POP3 server, you provide POP3 access to 602LAN SUITE user mailboxes via the POP3 protocol. You can also specify rules for collecting messages from POP3 mailboxes on the Internet and delivering them to 602LAN SUITE user mailboxes.



Enabling the POP3 and/or SSL POP3 Server

Use the switch box POP3 Server (enable POP3 access to 602Pro mailboxes) to enable or disable operation of the integrated POP3 server. It is possible to select the IP interface where the service will operate on. All interfaces are selected by default. You can choose one interface for the POP3 server from the POP3 server's IP address pull-down box. 602LAN SUITE also includes an SSL POP3 server that provides a secure server to client connection. Setup the SSL POP3 server just like the standard POP3 server (above). The default port where the SSL POP3 server listens is 995. In order to use SSL Security you must first generate an SSL certificate. See the SSL configuration section of this manual for details.

List of POP3 Mailboxes

Enter the POP3 account information into the input fields and click the Add button to create a collection rule. If you want to delete an item from the list, highlight the item and click the Delete/Edit button.

A mailbox on the Internet is identified by the address on which it is created (either in numerical or domain form) and by its name (or name of the user). Access is granted by the password, which was assigned to the user mailbox the moment it was created. Enter the corresponding values into the input fields:

- POP3 server (computer address)
- Login name (User Name)
- Password
- APOP login method

Setting the list box APOP login method to **Yes** gives you additionally protection to the mailbox host computer. The password is not sent at all. Only its imprint in a random string received from the server is returned for checking. It is up to the connection provider to inform you if their server supports this.

Routing Messages

Messages from a POP3 mailbox can be collected and automatically sorted to a local user mailbox:

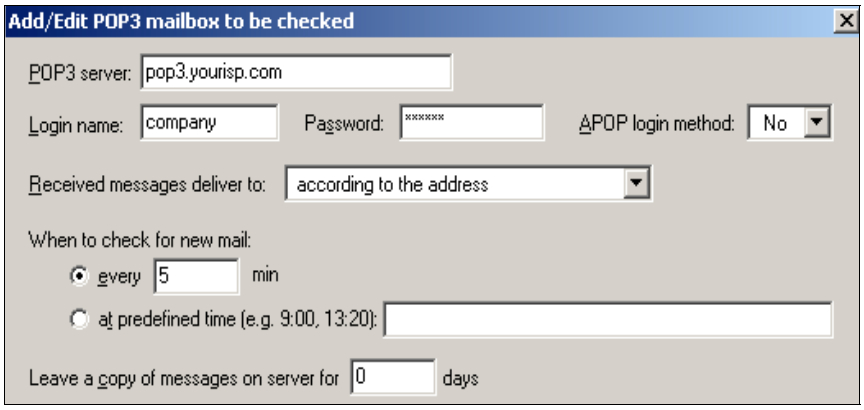
- According to the address – When your ISP routes all e-mail to a domain into one POP3 account (e.g. bob@company.com, john@company.com) this will automatically sort the e-mail to the specific user.

- According to the address – alternative method – Same as above, but uses different header analysis. Try this option if you are having problems with the first sorting method.
- To a specific user - To direct all collected e-mail from the POP3 account to a specific user, select the user from this list.

Mailbox Collection Interval

POP3 mailbox collection can occur in a set time that will be repeated or at specific times:

- **Every X minutes:** Enter the time interval in minutes you want to collect the POP3 mailbox contents.
- **At predefined times:** Enter times in 24-hour format separated with a comma when you want to collect the POP3 mailbox contents.


Add/Edit POP3 mailbox to be checked
POP3 server: pop3.yourisp.com
Login name: company
Password: ******
APOP login method: No
Received messages deliver to: according to the address
When to check for new mail:
every 5 min
at predefined time (e.g. 9:00, 13:20):
Leave a copy of messages on server for 0 days

NOTE: This interval can be more specific by using a global time restriction on the Connection tab.

Configuring Your Anti-virus Protection

602LAN SUITE Anti-virus Edition provides scanning of all messages for viruses using BitDefender Anti-virus technology. All e-mail messages and attachments will be scanned for malicious viruses and worms at the server before they reach your user's mailbox. The BitDefender engine is certified by ICSA Labs.

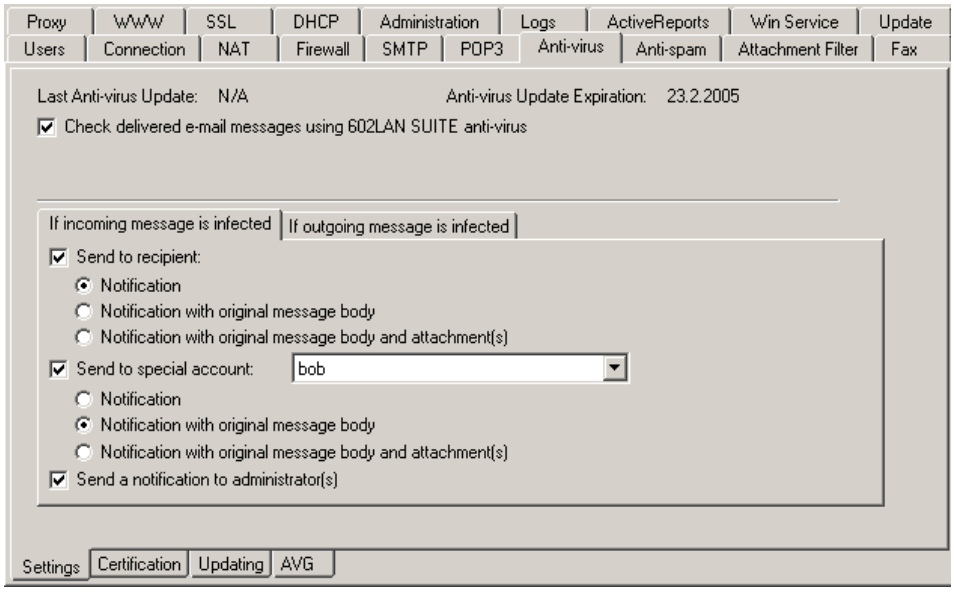
Seamless integration with BitDefender Anti-virus provides an enhanced virus warning system. All infected parts of an e-mail can be automatically removed, an e-mail notification to the recipient can be sent and the entire message can be delivered to a special account for later review. To enable scanning, check the Check delivered messages using 602LAN SUITE anti-virus checkbox on the Anti-virus tab. If the delivered message is infected, you have the following options:

- **Send to recipient**
  - Notification
  - Notification with original message body
  - Notification with original message body and attachment(s)
- **Send to special account** – select an account from the combo box
  - Notification
  - Notification with original message body
  - Notification with original message body and attachment(s)
- **Send a notification to administrator(s)**

Certification tab – All scanned e-mail can be stamped with a certification tag. Here you can enable certification if desired and define the certification message.

Updating tab – New viruses are released daily. To keep your virus protection up-to-date we recommend checking the **Enable automatic Anti-virus Updates** checkbox. It is possible to enter an interval in hours that you wish to update the virus database. If you want to update the virus database manually click the **Update Now** button.

AVG tab - 602LAN SUITE also supports anti-virus scanning from AVG available from Grisoft, Inc. If you have AVG installed on this computer and you want to scan delivered messages via AVG check the checkbox **Check delivered messages using AVG anti-virus**.



NOTE: 602LAN SUITE supports simultaneous scanning from 602LAN SUITE Anti-virus and AVG.

Configuring E-mail Client Access

602LAN SUITE supports the sending and retrieval of e-mail in two ways:

- The Use of a third party POP3/SMTP compliant e-mail program such as Microsoft Outlook, Outlook Express, Eudora, or similar.
- 602LAN SUITE Web Mail client

Here we will cover the setup of the two most popular e-mail clients, Microsoft® Outlook and Microsoft® Outlook Express. These instructions can also be used as a guide for setting up other POP3 e-mail clients.

Setting Up Microsoft® Outlook Express 6.x

1. Open Outlook Express
2. Enter your full name into the field labeled Display name, then click Next
3. Select I already have an e-mail address that I'd like to use, then enter your e-mail address into the field labeled E-mail address and then click Next
4. In the drop down list-box, select the server type as POP3, for Incoming Mail server and Outgoing mail server enter the IP of 602LAN SUITE (probably 192.168.1.1), then click Next

Setting Up Microsoft® Outlook 2002

1. Open Outlook 2002
2. Click Tools - E-mail Accounts
3. Select E-mail / Add a new e-mail account then click Next
4. Select POP3 then click Next
5. In the field labeled Your Name, enter the name to appear on all messages you send
6. In the field labeled E-mail Address, enter the e-mail address to appear as the sender address on all e-mail you send
7. In the field labeled Incoming mail server (POP3), enter the IP address of your server (probably 192.168.1.1).
8. In the field labeled Outgoing mail server (SMTP), enter the IP address of your server (probably 192.168.1.1).
9. Enter your 602LAN SUITE user ID in the field labeled User Name
10. Enter your 602LAN SUITE user password in the field labeled Password
11. Make sure the checkbox labeled Log on using Secure Password Authentication is NOT checked.
12. Click Next
13. Click Finish

Accessing the Web Mail Client

Run an Internet browser and enter the IP address or domain of the computer where 602LAN SUITE is running (i.e. http://192.168.1.1/mail or http://www.yourdomain.com/mail):

1. Enter your Username – This field is not case sensitive.
2. Enter your Password – This field is not case sensitive.
3. Click the Login button.

NOTE: If the SSL WWW server is enabled you may access the Web Mail Client via https instead of http.

Configuring Your Web Server

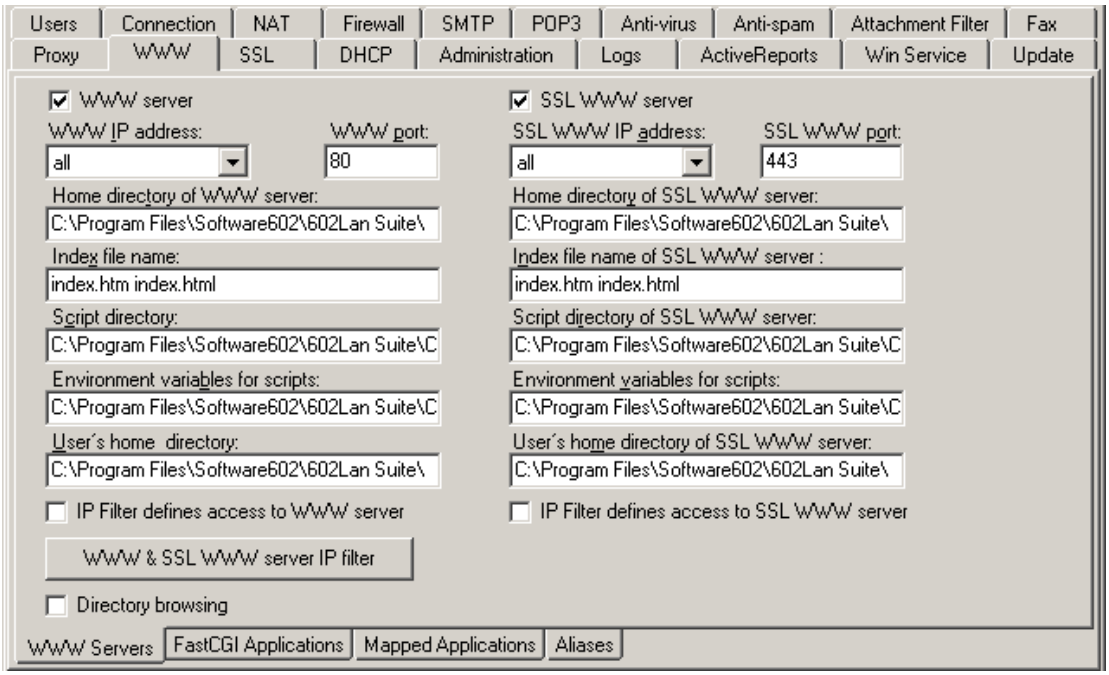
WWW Configuration

Check the box WWW server, if you want to use the functionality of the WWW server. It is possible to select the IP interface on which the WWW server will operate on from the WWW IP address checkbox. The default value is all interfaces but you can select a specific interface if needed. Use the field WWW port to specify the port allocated for communication with the WWW server (default value is 80).

NOTE: If you want to run a web server other than 602LAN SUITE's you will need to turn the web server off or change the port (i.e. 8080 – this will allow you to still access 602LAN SUITE's remote admin feature and not conflict with other web server software). The directories and files necessary to operate this server are specified in the five input fields.

To use the WWW server, you must specify the following:

- **Home directory of WWW server** - Path to the root directory in the field.
- **Index file name** - File name that will be used as the index page (e.g. index.htm or index.html
- **Script directory** - Directory with CGI or FastCGI scripts.
- **Environment variables for scripts** – Environment variables used with scripts.
- **User's home directory** - The directory path where personal user WWW pages will be placed.



Once the user's home directory has been defined, 602LAN SUITE will automatically create a sub-directory of the user name in this folder when a new user is created. In contrast to a typical Web server directory, user directories can only be accessed via http://computername/~username regardless of the folder setting. A user can update their home directory in the following ways:

- Copy files to the station where 602LAN SUITE is running to the appropriate user WWW folder (i.e. it must be shared).
- Upload the pages from Netscape Navigator or 602Text via the HTTP protocol after logging in with the correct username and password.
- Upload the pages via the FTP protocol – in this case the user WWW folders must be created as a subdirectories off the main WWW directory (User's home directory on the WWW tab).

602LAN SUITE also includes an SSL WWW server that provides a secure server to client connection. Setup the SSL WWW server just like the standard WWW server (above). The default port where the SSL WWW server listens is 443. You will need to generate a self-signed certificate or install a purchased certificate from a reputable Certificate Authority such as Verisign or Thawte. The benefits to purchasing a certificate are that all browsers will globally recognize your certificate and automatically trust your site security. A self-signed certificate will prompt the user that the certificate is not recognized but the site is still secure. Both certificates provide equal protection.

Using User Folders

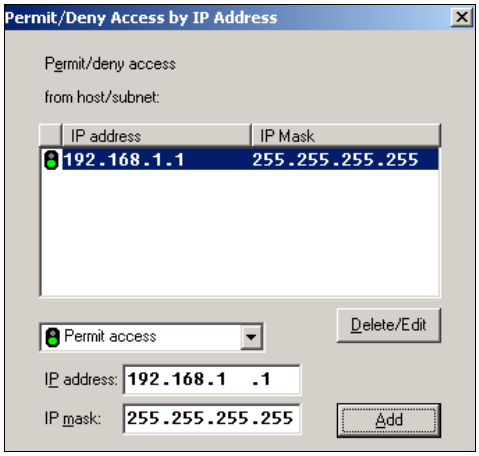
Each user has his/her own User's home directory on the WWW server where they can publish information. The user folders are accessible from an Internet browser via http://computername/~username where computername is the name/IP address of the computer where 602LAN SUITE is running and username is the name of the user folder that equals the user's username.
Users can update their pages via the following methods:

- Copying files directly to the fileserver where the user folders are located.
- Update pages via HTTP from Netscape Navigator. It requires a proper login (user name and password).
- Via the FTP protocol – access to the user folder from an FTP client. It is necessary to enter the computername, username and user password.

If the user is not an administrator, him/her will access their user folder.
If the user is an administrator, him/her will access the root of the WWW server.

Access Filter

By checking the box IP filter defines access to WWW server the WWW & SSL WWW IP filter will define access to the WWW server. The IP filter rules are checked from top to bottom with each rule superceding those above it. Enter the IP address and mask of the computer or network that sends the request to the field IP address and IP mask. It is also necessary to define if the item is allowed or prohibited – RED means access denied, GREEN means permit access.



Directory Browsing

By checking the Directory browsing checkbox you can enable Directory browsing on the web server. This will allow web visitors to browse directories on your web server that do not include an index page.

Updating Web Server Content

You can update web server content in one of two ways:

- Locally
- Remotely via FTP

Updating from the local server

Update web site content by copying the updated files to the home directory as you have specified on the WWW Tab. By default, the home directory is the DOCS folder under the 602LAN SUITE folder.

Updating remotely via FTP

The most popular form of web server updating is transferring files via the FTP protocol. In order to perform this there are a few pre-requisites:

- You must have the "allow update of WWW server via FTP port xx" option selected on the administration tab.
- You must be an administrator to access the home folder of the WWW server. Standard users can only access their own private folders.

Use an FTP client to connect and login to the 602LAN SUITE WWW server. Administrators will default to the home directory while standard users will default to their private folder. Please refer to your individual FTP client for uploading instructions. Internet Explorer can be used as an FTP client. To access through MSIE, do the following:

1. Type in ftp://yourserver.com where your server.com is the domain or IP address of your 602LAN SUITE server.
2. You will be prompted to login with a user name and password, enter these appropriately (Anonymous login is not supported)
3. You will now be taken to the home directory if you logged in as an administrator or to your personal folder if you logged in as a regular user.
4. Use standard copy and paste commands to transfer files between your computer and the FTP site.

Setting Up an SSL Web Server

To enable the SSL web server simply check the SSL WWW Server selection on the WWW tab. You must have an SSL certificate defined in order to save the changes. For information on creating or installing an SSL certificate, see the Advanced Access Control section of this manual. The SSL web server has it's own configurable parameters which are identical to the standard web server. This allows you the option of selecting a different home directory for secure documents you may be distributing over the Internet.

The SSL web server gives you the following benefits:

- Use the 602LAN SUITE web mail client via a secure SSL connection to ensure the privacy of your e-mail. Example: https://yourserver/mail.
- Secure the remote administration of your 602LAN SUITE by simply using https in place of http in your remote administration address. Example: https://yourserver/admin

FastCGI Applications

To use a FastCGI application, register the application by defining the following values:

- **FastCGI application name** – Application name that will be presented in the list.
- **Role** – The FastCGI Application can process several types of requests (it can have several roles). Here you have to specify which role you have in mind. If you do not have a specially programmed application, the role should equal 1 (the FastCGI application returns the HTML page that corresponds to the particular path). The following roles are pre-defined: Responder, Authorizer and Filter.
- **Location (URL)** – Location (path) that the user specifies in the WWW browser for calling this FastCGI application.
- **Connection (address:port)** – It is necessary to specify the computer and port on which the current FastCGI application is running. If the application is running on the local computer, you can specify only the <port number> or localhost:<port number>.
- **Path to EXE file** – If the executable file of the FastCGI application is on this computer, the WWW server can open this file during start-up so that it is ready to process a request.

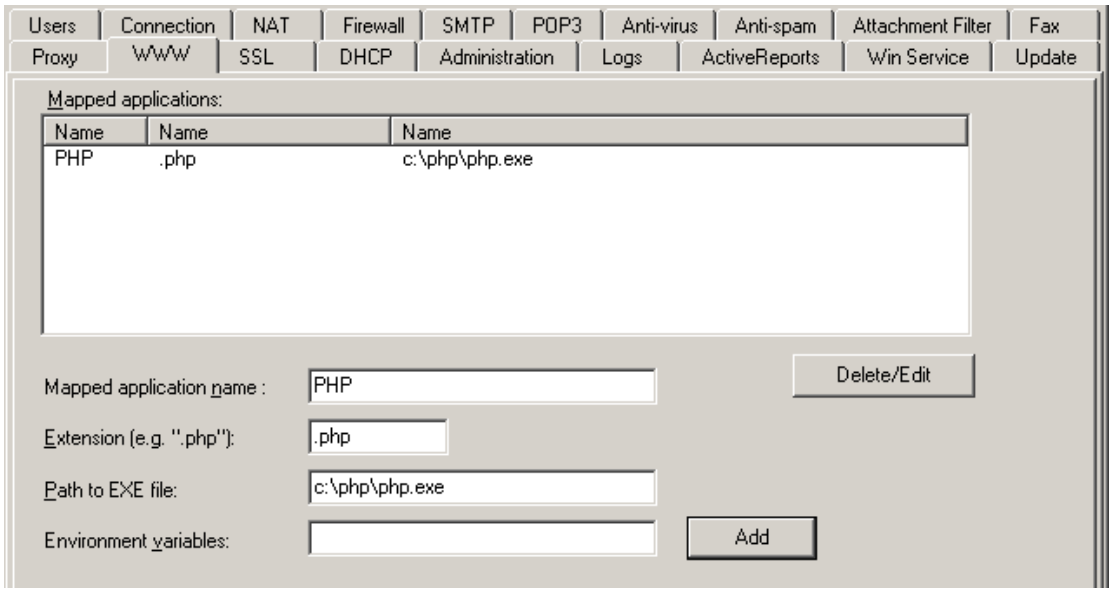
- **Environment variables** – The FastCGI application receives complete information from the WWW server about the established connection and server type. Give their list in the following format: variable_name=value. Separate each variable with a semicolon.

For more information on FastCGI, see the WWW page: http://www.fastcgi.com.

Mapped Applications

If the WWW server finds the extension entered in the Extension field from the requested URL, it will run the application from the Path to EXE file field. To use a Mapped application, register the application by defining the following values:

- **Mapped application name** – Application name that will be presented in the list.
- **Extension** – Enter the file extension (e.g. .php).
- **Path to EXE file** – Enter the application EXE file name with full path. The WWW server will run this application upon URL request with the included extension entered in the extension field.
- **Environment variables** – It is possible to run the mapped application with specific parameters. Separate each parameter with a semicolon.



Aliases

To use aliases on the web server, define them by the following values:

- **Path** – Define the local path you would like to alias.
- **Alias** – Define the Alias as to how it will be accessible from the WWW server.
- **Environment variables** – It is possible to include an application (EXE file) to the URL request. Separate each parameter with a semicolon.

Configuring Your Fax Server

The Fax tab is used to set parameters that control sending and receiving fax messages. Faxes can be sent out through a fax modem. This configuration tab has two sub tabs:

- **General:** Used for general settings.
- **TAPI:** Used to setup the TAPI device (fax modem).

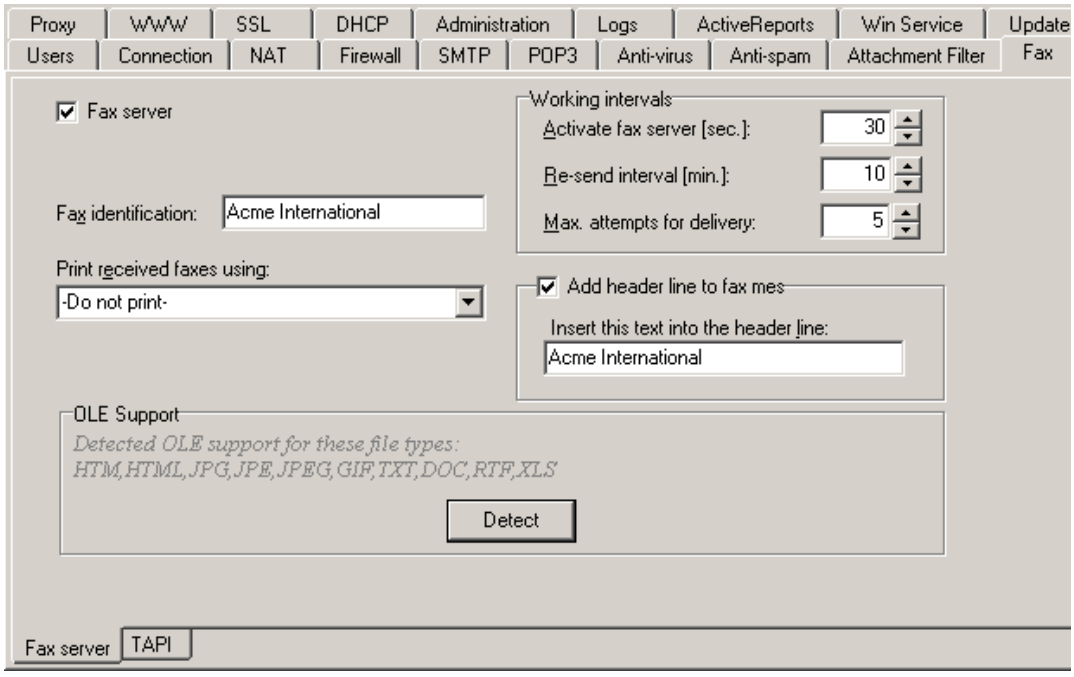
General
This tab sets up the method of faxing and its working intervals.

Fax Identification
Enter a string into the field Fax identification that includes the identification information about the fax sender. This information is transmitted to the counterpart fax machine during the first stage of transmission and allows the receiving party to identify you. This should include your fax number.

Print Received Faxes to a Printer
If you wish to print all incoming faxes to a printer, select a printer from the Print received faxes using pull-down menu and all incoming faxes will be printed to this printer.

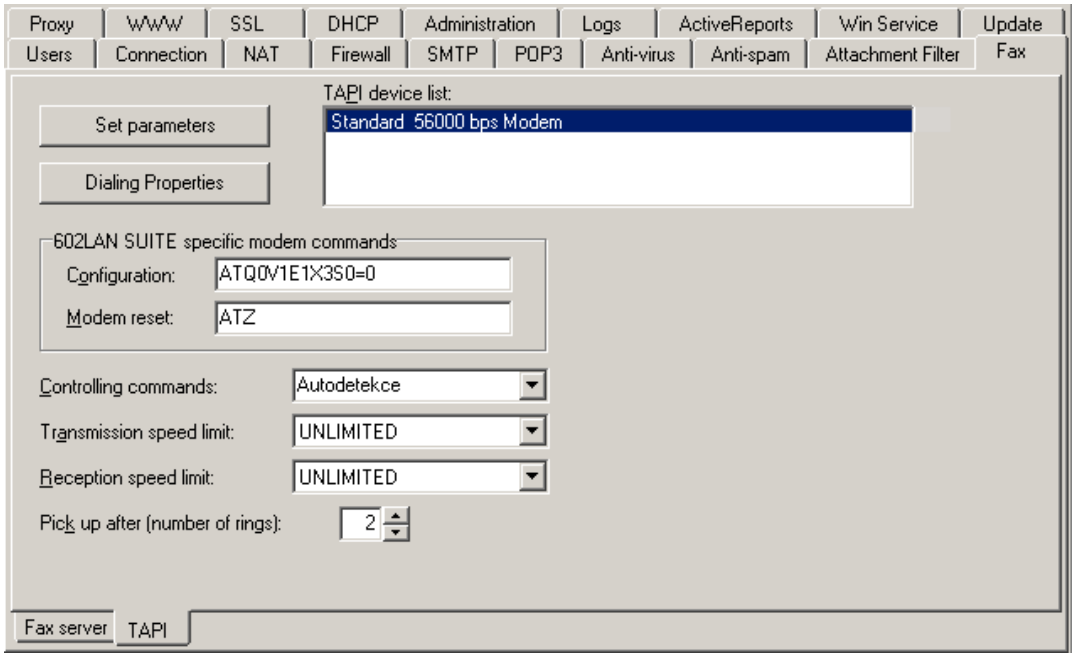
Working Intervals
This section sets the time interval for handling the communication events:
- **Activate Fax Server:** The fax server will check the fax queue every xx seconds and it will try to send one fax message.
- **Re-send interval:** If a sending attempt was unsuccessful, the server will send the unsuccessful fax message after the entered amount of minutes.
- **Max. attempts for delivery:** Defines the number of times to attempt delivery. The first sending attempt consists of four dial attempts and the next sending attempt will consist of two dial attempts.

Add Text to the Header line – Header Line Text
It is possible to enter a message into the field Header line text that will be printed as the first thing on a fax message. This information can include, for example, your identification.



TAPI
This tab sets the TAPI device parameters. All available TAPI devices are listed in the TAPI device list.

Set Parameters and Dialing Properties
Set parameters and the Dialing properties buttons open configuration dialog windows from the Windows Operating System. It is also possible to open these windows from Windows Control panel / Modem settings.



Modem Commands

- **Configuration** – Modem commands to configure your modem for 602LAN SUITE.
- **Modem reset** – Modem commands to reset your modem.

Controlling Commands

Fax modems have several sets of control commands in their fax section. The option Controlling Commands enables you to select this set directly or let the server attempt auto-detection.

- **Class 1:** The oldest of the three classes, lets the computer carry out most of the fax operations and thus leaves most of the operation up to the computer This set was arranged into a standard and therefore is frequently implemented in fax modems and control programs. The original standard did not include a definition of how the modem should distinguish a data call from a fax call when receiving a message. Older types of US Robotics modems support Class 1. Class 1 and Class 2 are supported by all modems based on the ROCKWELL chipset.
- **Class 2:** The fax modem carries out a number of communication operations (checking for a common protocol with the counterpart fax, page confirmation, transmission termination) itself or as a response to a single AT command. This set was never arranged into a standard; it was only formed as a set of recommendations that manufacturers sometimes did not adhere exactly to. This is the reason why there are some problems with this class. Differentiation between fax and data is not clearly defined here. This set is widely used with fax modems. ZyXEL supports this class in all FW versions, US Robotics has not implemented this class because it is not an official standard.
- **Class 2.0:** The latest version, with its structure of commands and method of operation, is very much like Class 2, but the commands are shorter and there are some extra commands that solve the problems

with Class 2. This set is fully standardized and is not widely used yet, but its popularity is increasing. ZyXEL Elite, ZyXEL 1496 FW 6.12+ and US Robotics support this standard. ROCKWELL does not support it.

Transmission and Reception Speed Limit

Transmission speed limit and Reception speed limit enable you to decrease the maximum fax transmission speed to the specified limit and thus adjust it to the line quality. There is a standard range of speeds from 2,400 to 14,400 bit/s or select the unlimited speed.

Pick Up After Number of Rings

The entry in Pick up after (number of rings) specifies the number of rings after which the server answers the incoming call.

SendFax Client Installation

If you want to fax out directly from any application providing the print function, it is necessary to install the SendFax print driver on the client workstations.

1. Download the SendFax Client from http://www.software602.com/download/
2. Run the installation program from the directory where you downloaded the program. Follow the directions given by the installation program.
3. After accepting the license agreement enter, **Name** – Your name, **Company** – Enter the name of the company where the server will be installed.
4. You must enter the directory where SendFax will be installed on the next screen.
5. At the end of installation all program files will be copied onto your hard drive and a new printer driver will be available to you.

Send a Fax with the SendFax Client

If you want to send a fax message directly from an application that provides the print function (i.e. MS Word), compose a document by the application and print to the Fax602 – fax for Windows print driver. The SendFax Print Driver creates a fax message and the window of the address book selected in the SendFax Print Driver configuration appears. After entering the recipient address or selecting a pre-existing recipient, the fax is sent to 602LAN SUITE. To send a fax, do the following:

1. Any Windows program with the Print function can be used. From any Windows program click File, Print... then select the Fax602 Printer. The 602Send Fax dialog window appears. Here you can enter a recipient manually or click the Select recipient(s) from the list button and select recipients.
2. Now select the page length and check Preview before sending if you want to see what the fax is going to look like before it is delivered.
3. Select the recipient(s).
4. Preview the fax (if the option was selected).
5. Click Send when ready.

Send a Fax by E-mail

If you want to send a fax message directly from an e-mail client, the only thing you have to do is enter the fax address in the e-mail format: fax_number@fax.fax or fax_number@fax. The fax number must always be entered in one of these two permitted formats. A fax is then created as a normal e-mail letter. 602LAN SUITE then recognizes the fax message due to the fax or fax.fax part of the e-mail address, compiles the message into the fax format and sends it. According to the server configuration it is also possible to attach files to a fax (DOC, WPD, RTF, HTML, etc.), check the Fax tab in 602LAN SUITE for a list of all support file types on your system.

Phone Number Format of E-mail Address

For sending faxes it is necessary to enter the fax address in the e-mail format: fax_number@fax.fax or fax_number@fax. The fax number part of the e-mail address must be entered in one of the two permitted formats: Full format or Direct format.

Full format - The full format of a phone number always includes the country code, area code and the number itself, separated with dashes.

The number cannot include a zero for reaching an outside line, long distance calls or international calls. To use the full format, it is necessary to set the Dialing properties and Location in the Windows Operating System properly (Check Fax tab / TAPI / Dialing Properties). Here you must enter all dialing properties:

- Country
- Area code
- For local calls dial
- For long distance calls dial

The phone number that you entered in the e-mail address is compared with the dialing properties.

- If your dialing properties include United States as the Country, 904 as the area code and the number dialed is different from the 904 Area code (i.e. 305), the number 13056667777 will be called.
- If your dialing properties include United States as the Country, 904 as the area code and the number dialed is from the same Area code, the local number 6667777 will be called.

Example 1: 1-904-6667777@fax
Example 2: 1-212-5559999@fax

Direct format - The number is written before the @ symbol exactly as it is to be dialed. The number must not include dashes, parenthesizes, pluses, spaces or other formatting symbols! Enter the number part exactly as you would use a phone!

Example 1: 6667777@fax
Example 2: 13056667777@fax

Send a Fax by E-mail with an Attachment

The letter you want to send and files attached to it must be converted into a graphic fax format. The transfer can be executed directly on the workstation by the 602LAN SUITE SendFax program or on the 602LAN SUITE Server. The server has a wide range of formats for the conversion process:

- **Internal conversion functions** – For conversion of text files and graphic bitmap files. Internally supported file formats: TXT, BMP, CLP, DCX, DIB, GIF, CUT, JPG, PCX, TIF, WMF.
- **External functions** – For conversion of certain file formats into the fax format by background printing through the Fax602 fax driver.

Externally supported file formats depends on programs that are installed on the workstation with the 602LAN SUITE Server:

- **DOC:** Word7 or later, 602Text
- **XLS:** Excel97 or later
- **WPD:** 602Text
- **RTF:** Word7 or later
- **HTM, HTML:** MSIE 4 or later, Word97 or later

The currently supported external formats are displayed under Settings / Advanced Configuration / Fax tab of the 602LAN SUITE Server.

NOTE: In some applications it is necessary to set the Fax602 driver as the default printer.

Configuring Shared Internet Access

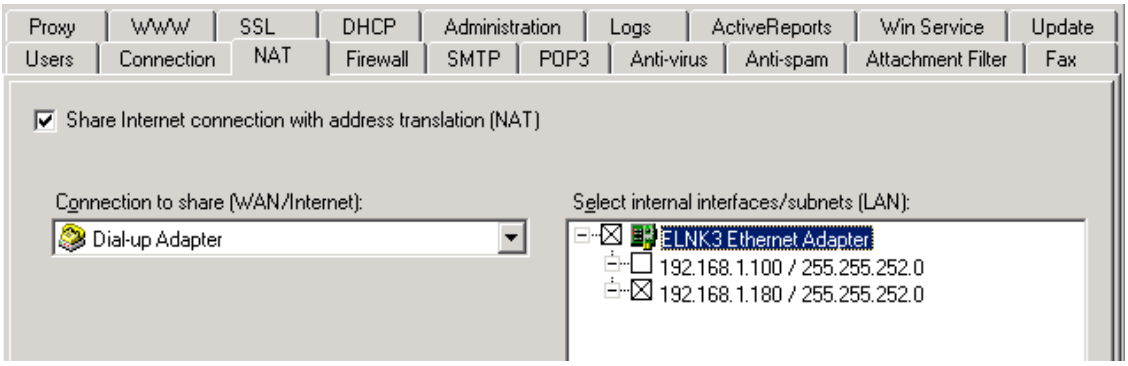
To configure shared Internet access through 602LAN SUITE you must first configure the server to allow network address translation and then the client's TCP/IP gateway must be set to the IP address of the computer running 602LAN SUITE. If you wish to use user authentication or site access control, then you will need to use the proxy services described in the "Proxy" section under the "Advanced Access Control" chapter of the manual.

What is Network Address Translation (NAT)?

NAT is the translation of an Internet Protocol address (IP address) used within one network (your private network) to a different IP address known within another network (the Internet). NAT maps local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back to the local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves the number of global IP addresses needed and allows the use of a single IP address to communicate with the Internet.

Enabling NAT

NAT requires that at least two interfaces be installed on the computer where 602LAN SUITE is running (e.g. two NICs or a NIC and a Dial-up adapter). To begin using NAT in 602LAN SUITE you must first check the box in the upper left had corner of the NAT tab. Next, select the connection you wish to share in the "Connection to share" box. Now, select the internal network(s) from the "Select internal interfaces/subnets" box to define what network(s) will be allowed to access NAT. If an interface has more than one IP address you can select individual addresses according to your needs.



Setting Up Client Access Through NAT

The client computer's TCP/IP setting can be set either manually or automatically via DHCP. Manual configuration requires IP addresses to be set from the same network as the 602LAN SUITE internal interface (e.g. 192.168.1.x) and this internal interface must be entered into the TCP/IP gateway settings as part of the TCP/IP settings (e.g. 192.168.1.1).

To configure TCP/IP by DHCP, see the section "DHCP Server Setup" under the "Basic Administration" chapter.

NAT Example

A computer with 602LAN SUITE has one internal interface with the IP address 192.168.1.1 and 255.255.255.0 mask. Workstations that need access to 602LAN SUITE's NAT must be configured in the following way:

- IP address: 192.168.1.x (where x is a number from 2 - 254)
- Mask: 255.255.255.0
- Gateway: 192.168.1.1

NAT IP Filter

The NAT IP Filter defines what connections are allowed to access NAT. The IP filter rules are checked from top to bottom with each rule superceding those above it. Enter the IP address and mask of the computer or network that sends the request to the field IP address and IP mask. It is also necessary to define if the item is allowed or prohibited – RED means access denied, GREEN means permit access. If the IP filter includes a rule, all data transmission is prohibited except transmission defined by this rule. If the IP filter does not contain a rule, all data transmission is allowed.

NAT Limitations

- NAT does NOT support tracert, NetMeeting, IPsec or UPnP.
- NAT does NOT work on servers with multiple processors or processors with Hyper-threading.
- NAT will NOT establish a dial-up connection.

Basic Administration

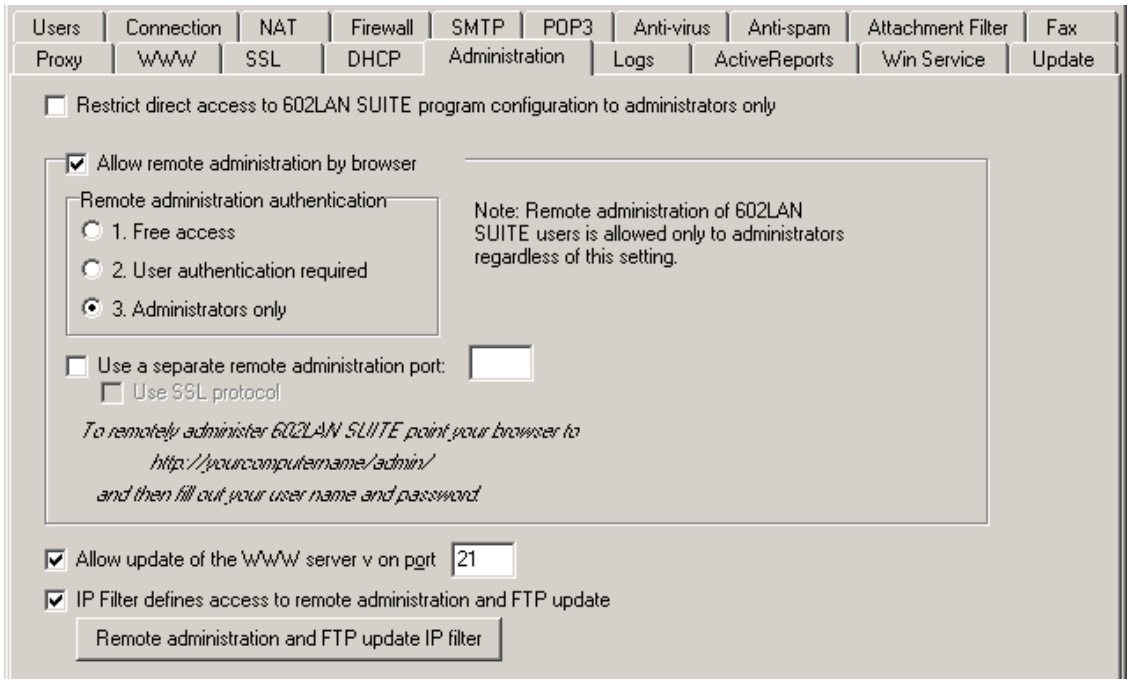
602LAN SUITE can be administered via two different administration methods:

- The application
- The web based administration utility

While both of these methods have similar capabilities, each one has its own merits.

Administration Configuration

Administration options are configured on the Administration tab. To enable remote web administration, check the Allow remote administration by browser checkbox. If a user with the admin right exists, it is possible to restrict direct access to the program configuration to administrators only. If no administrators are defined, this checkbox is not available.



Administration via the Application

This option provides you with total unrestricted access to all of 602LAN SUITE's administration options including the ability to modify service parameters and govern administration options. The disadvantage to this is that you must be physically sitting at the server or utilizing remote PC access in order to administer via this method.

Web Based Administration

Web based administration offers the administrator the convenience of being able to change settings, modify users and change service parameters within the 602LAN SUITE program from any PC on the local network or if properly setup, any Internet connected PC in the world. The drawback to this convenience is that you will not have access to the administration control options or the Windows Service parameters. This is generally not a problem, as day-to-day administration typically does not utilize them. They will be setup once and generally be left alone for the remainder of the program's service life.

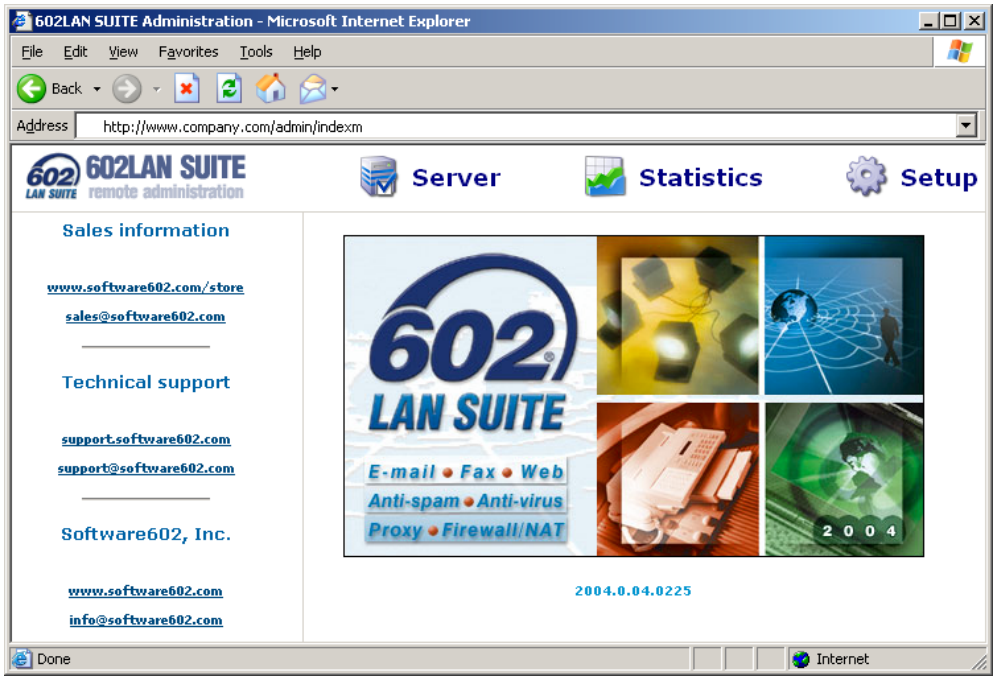
© 2004 Software602, Inc. 9/2004

NOTE: If you are using 602LAN SUITE as a Windows Service, you must either use the web-based administration to administer your 602LAN SUITE program or stop the service before opening the application.

Accessing the Web Based Administration Utility

To access the remote administration utility, you must open the browser on any network connected PC and then enter the following address while substituting "yourservername" for the 602LAN SUITE server's IP address, registered domain name or computer name:

http://yourservername/admin



Upon establishing a connection to the 602LAN SUITE WWW server, you will be prompted for a user name and password. Access to the remote administration can be restricted to "Administrators only" on the Administration tab; otherwise, all valid 602LAN SUITE users will have access to the remote administration.

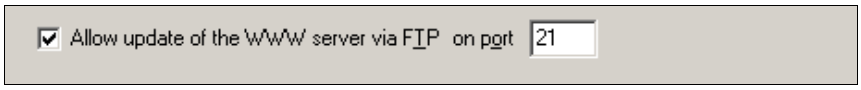
NOTE: If you want to use the IP Filter rules to secure remote administration and prevent outside or unauthorized IP addresses from being able to access, check the IP Filter defines access to remote administration and FTP update checkbox.

WWW Server and Web Based Administration

Remote administration runs on 602LAN SUITE's built in WWW server and therefore must follow rules set forth in the WWW tab. If your WWW tab is set to only allow access on the internal network interface, then Remote administration will be available only to clients accessing via the internal network. If you have the WWW server set to allow access on all interfaces, the administrator may administer 602LAN SUITE from any Internet connected PC. In addition to the interface settings, Remote Administration is also subject to the rules enforced by the IP Filter on the WWW tab.

Updating the WWW server via FTP

HTML pages on the 602LAN SUITE WWW server are stored in the folder that is defined on the WWW tab. The default folder is /DOCS. It is possible to maintain them directly or you can do this remotely via the HTTP or FTP protocols as well. To allow updates to the HTML pages via FTP, check the Allow update of the WWW server via FTP on port xxx checkbox on the Administration tab. The standard FTP port is 21.



NOTE: To run an FTP server other than 602LAN SUITE's, use a different port (i.e. 8021 – This will allow access to 602LAN SUITE's FTP service and not conflict with other FTP server software).

There are Several Ways to Manage HTML Pages on the WWW Server

It is possible to send HTML pages via any FTP client to the 602LAN SUITE FTP Server:

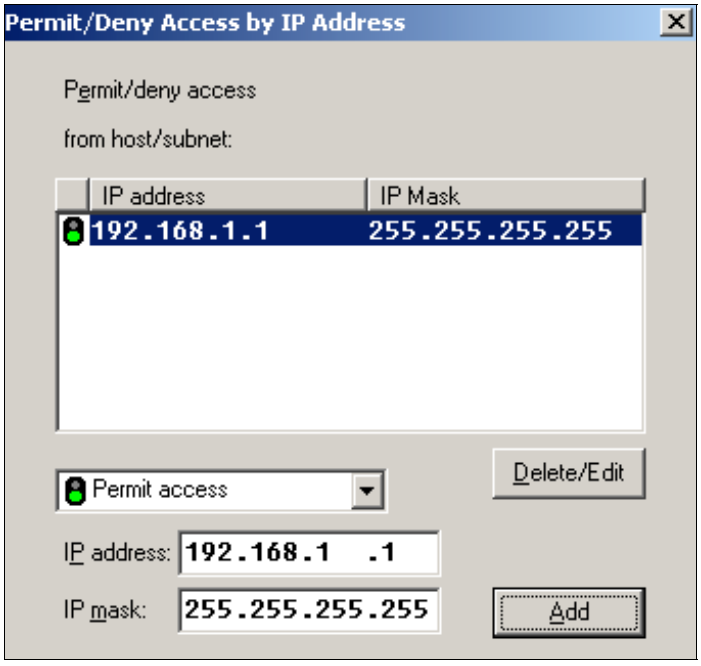
- If you use Netscape Navigator, use its HTML editor (Netscape Composer) and use the Publish icon – protocol HTTP PUT.
- If you use Microsoft Internet Explorer, use the Web Publishing Wizard (default Windows 98, MSIE 4.0 or higher, FrontPage) – HTML pages will be sent via the FTP protocol.

Who is permitted to manage the WWW Server

Only 602LAN SUITE administrators are permitted to manage the 602LAN SUITE WWW server. Other users are only permitted to update their personal pages.

Remote Administration and FTP Update IP Filter

The Remote administration and FTP update IP filter defines what connections are allowed to access the web administration and FTP update server. The IP filter rules are checked from top to bottom with each rule superceding those above it. Enter the IP address and mask of the computer or network that sends the request to the field IP address and IP mask. It is also necessary to define if the item is allowed or prohibited – RED means access denied, GREEN means permit access.

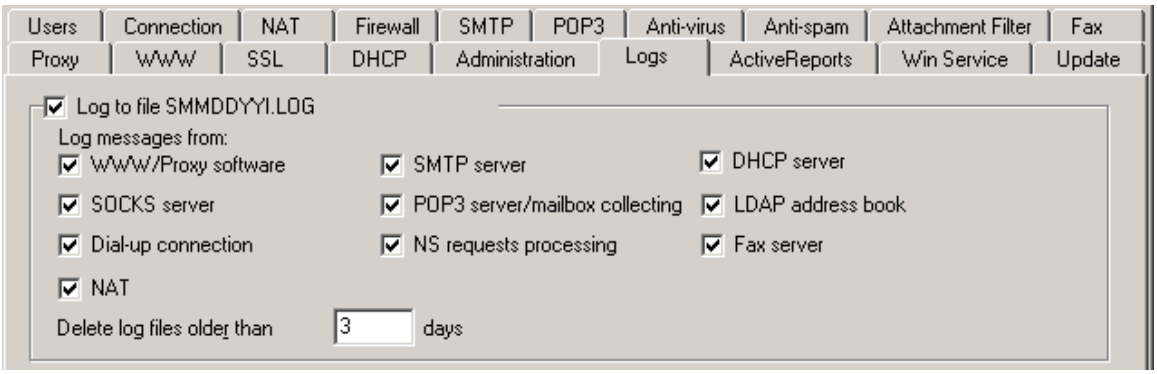


Logging Server Activity

Logs Tab

Reports of the server's activity are shown by default in the program window and can be logged to a file. 602LAN SUITE provides logging WWW and HTTP proxy server activities in the W3C format for later analysis by W3C log file analyzers.

- **Number of lines in the terminal buffer:** Specify the number of lines that will be stored in memory (i.e. how far back you will be able to scroll up in the program window).
- **Log to file:** Reports the server's activity to a file. Check the box Log to File, to generate a log file for each day. The file can be found in the 602LAN SUITE directory, with the name SMMDDYYI.LOG (MM means months, DD means day and YY means the last two digits of the year). Each file is stored for the number of days specified in Delete log files older than x days, after which the file is deleted.
- **Maximum size of statistics log file in kB:** Another log file is available: lansuite.csv. This file is automatically created after sending the first fax message and only logs sent faxes. The maximum size of the CSV file is limited to the value specified in Maximum size of statistics log file in kB. After reaching the entered size, the CSV file will be cut by 10 percent and logging will continue.



Use the section Log messages from to specify the services to monitor reports from:

- WWW/Proxy software
- SOCKS server
- Dial-up connection
- NS requests processing
- DHCP Server
- SMTP server
- POP3 server/mailbox collecting
- LDAP Address Book
- Fax server

W3C – Extended Log File Format

Most web servers offer the option to store log files in either the common log format (http://www.w3.org/Daemon/User/Config/Logging.html#common-logfile-format) or a proprietary format. 602LAN SUITE provides the following log files in the W3C - extended log file format:

- **W3CA.LOG** - WWW server log file
- **W3CP.LOG** - Proxy server log file
- **W3CC.LOG** - Cache Proxy server log file

W3C log files are recorded in a format readable by analysis tools. A header specifying the data type is recorded at the beginning of each log file.

Firewall messages
Firewall messages will be logged to the FW.LOG file. The options that are checked will define what will be logged to the file. Here is a description of the options:

- Log dropped packets – Dropped packets will be logged.
- Log packets starting & ending – The beginning and end of each TCP connection.
- Log all packets – All traffic will be logged (**WARNING**: Should only be used for debugging purposes!).

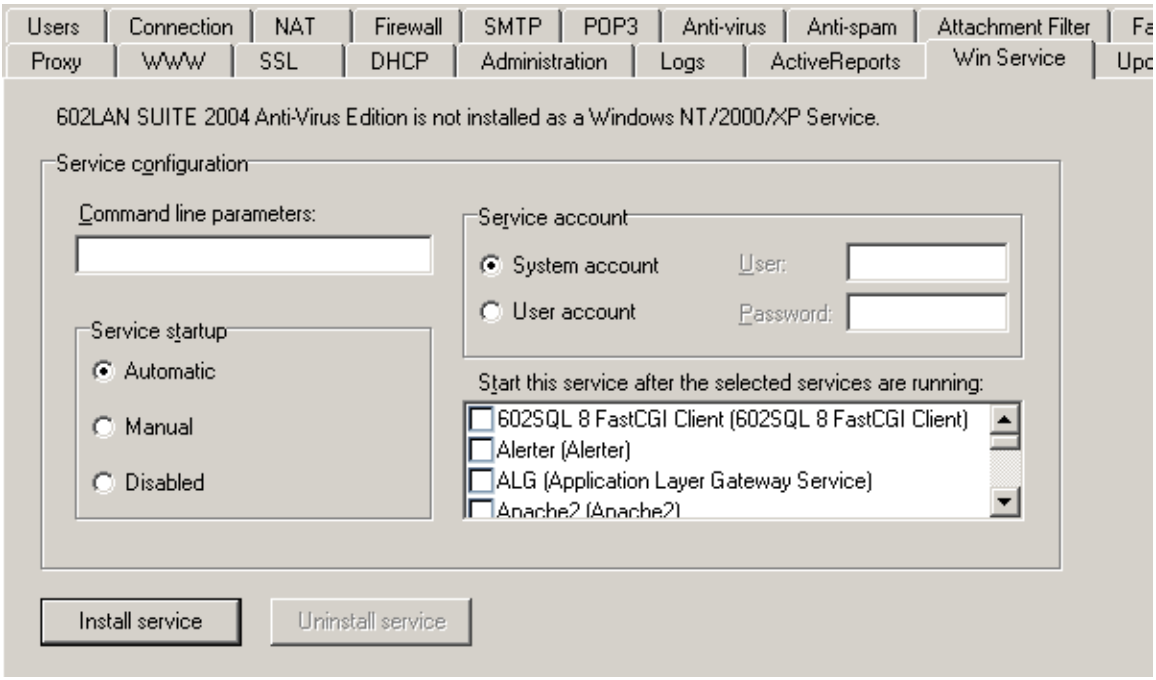
Installing as a Windows Service

NT Service

The NT Service tab is displayed if the operating system is Windows NT/2000/XP/2003. This tab allows you to control the 602LAN SUITE service. Other elements of this dialog box enable the program to be installed as a service or to modify settings for the service:

- **Command line parameters** – Here the command line parameters are entered that will be used at service startup.
- **Service commands** – Here you can specify if the service should start automatically at system startup or if the user must start it manually from Windows / Control Panel / Services, or if the service should be disabled.
- **Service account** – An account is assigned to the service upon startup that determines what rights the service can utilize. For example, if 602LAN SUITE needs access to disks on another computer, you must specify an account of a user who has the right to access these disks.
- **Start service after selected services are running** – Sometimes it is necessary to guarantee that one or more service is loaded before 602LAN SUITE is started. Here you can specify these services and 602LAN SUITE will start after the selected services are in operation.

After changing the settings, click the Install Service button to install 602LAN SUITE as a service. Use the button Uninstall Service to uninstall the service.



NOTE: This will not affect the current status of the service (e.g. if 602LAN SUITE is currently started as a service you will need to stop it manually).

Win98 Service

If you use Windows 9x the Win98 service tab will appear. Here you can setup 602LAN SUITE as a Win98 service. The text at the top will state if the Win98 service is installed or not. The term Win98 service means you can automatically run 602LAN SUITE at startup. Its icon is hidden in the bottom right-hand corner of the screen (System Tray). Enter the command line parameters in the Command line parameter field that need to be used (Optional). To setup 602LAN SUITE as a Win98 service, click Install service. To uninstall it, click Uninstall service.

DHCP Server Setup

DHCP (Dynamic Host Configuration Protocol) provides basic TCP/IP settings for network workstations. Workstations can use the DHCP server to obtain an IP address, mask, DNS and more. Dynamic IP assignment means easy administration and it also conserves assigned IP's to the amount of in-use working workstations only. DHCP uses the UDP protocol on port 67 and 68. DHCP is an open standard, developed by the Dynamic Host Configuration working group (DHC WG) of the Internet Engineering task Force (IETF). The DHCP protocol is derived from RARP, DRARP and BOOTP protocols. A full description can be found in RFC 2131, 1531, 1541, 1534, and 2132.

Turning on the DHCP Server

To begin using the DHCP server in 602LAN SUITE you must first check the box in the upper left had corner of the DHCP server window. Also make sure that the IP address of the INTERNAL network is selected for the option DHCP server's IP address.

Setting the IP Range

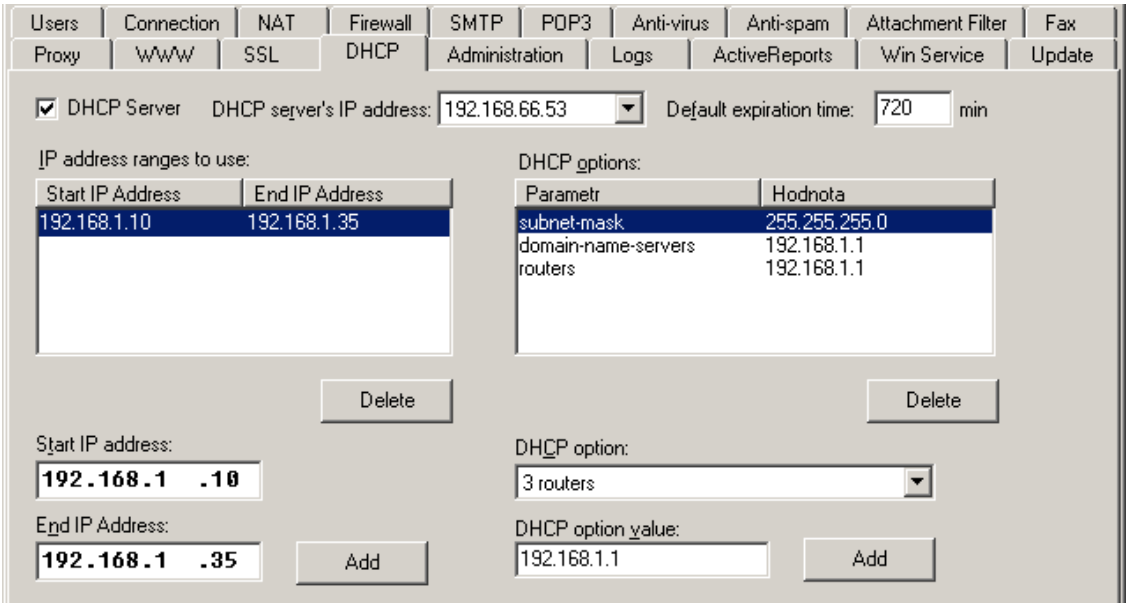
Next you will need to define a Start IP address and an End IP Address. We suggest using Class C IP address such as 192.168.x.x. The Start IP address should be 192.168.1.10 and your End IP address can be up to 192.168.1.254. Once those are entered click Add. To delete any interval, highlight the interval and press the Delete button. Starting with 192.168.1.10 you give yourself 9 IP address to use on servers and PCs you wish to not use DHCP. These IP address are 192.168.1.1 - 192.168.1.9. Multiple intervals can be defined.

DHCP Options

There are many DHCP options and variables supported in 602LAN SUITE, but you only need 3:

- **subnet-mask:** This should be set to 255.255.255.0
- **domain-name-servers:** This should be set to the IP address of the computer running 602LAN SUITE (with the DNS proxy enabled).
- **routers:** This should be set to the IP address of the computer running 602LAN SUITE (with NAT enabled)

Select the appropriate DHCP parameter and enter the DHCP option value then click the Add button. To delete any parameter, highlight the parameter and press the Delete button. For more information on DHCP and its options and variables please visit http://www.dhcp.org.



Advanced Features

SMTP Authentication & Settings

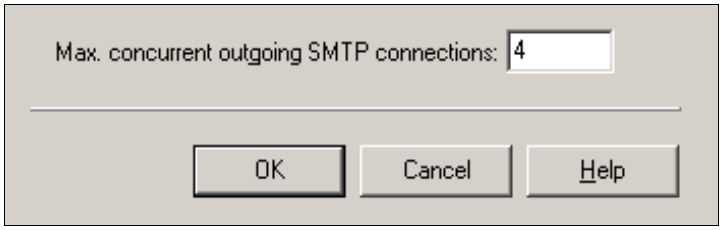
Advanced Sending Parameters Settings
Some ISP's require authentication to send e-mail via their SMTP server. If your ISP requires this, check the ISP's SMTP server requires authentication. Select the authentication method - SMTP or POP3 (ask your provider) and fill out your Login name and Password.

Private Networks
Routing messages according to the Preset routes settings is available in case you need to send messages for specific domains to specific computers instead of to the Internet. The Preset routes button is enabled if you check the Use preset routes check box. After pushing the Preset routes button, the list of preset routes will appear. Enter the values you need to Mail domain and Destination host fields then click the add button. You can edit or delete all of the entered values. Simply highlight the appropriate value and push the Delete/Edit button.

DNS Service Settings
Enter the IP address of your DNS (this was assigned to you by your Internet Provider) into the field DNS1 and DNS2 (if available). If these fields are left empty, 602LAN SUITE will use the DNS settings from the TCP/IP configuration in Windows (see Sending outgoing messages directly to the Internet using DNS above).

Working Intervals
Working Intervals includes a group of fields used to set SMTP time intervals. If the message cannot be sent (i.e. the destination SMTP server is offline), an attempt will be repeated after a certain period. Specify this delay by entering the number of minutes into the field Re-send Interval.

Max concurrent outgoing SMTP connections
This determines the maximum number of simultaneous outgoing SMTP connections. If you are processing a large volume of e-mail through 602LAN SUITE, raising this number will allow outgoing messages to process faster provided adequate bandwidth is available.



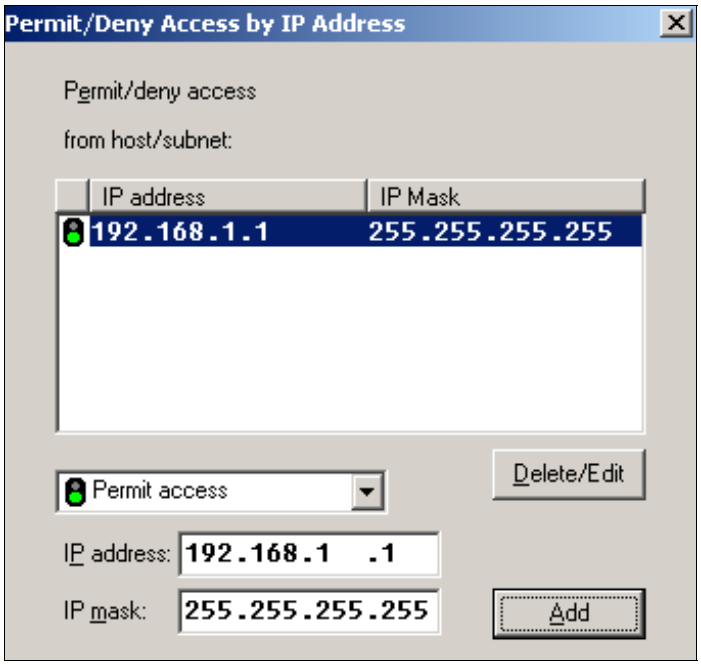
HELO/EHLO command parameter
Here you can enter a fully qualified domain name you want to send to remote SMTP servers.

SMTP Relay Options
SMTP relay functions provide message routing for recipient(s) (i.e. the address in the TO: field) that do not have an account (mailbox) on the 602LAN SUITE server. This function is necessary for 602LAN SUITE users since they send messages from an SMTP/POP3 client application (Eudora, Outlook Express) to 602LAN SUITE (from which 602LAN SUITE then forwards to the Internet). By default, 602LAN SUITE's SMTP Server will only work for 602LAN SUITE users (check Relay for 602LAN SUITE users only). The SMTP server will check the Internet address of the sender (i.e. the address in the FROM: field) and if the user's e-mail address does not correspond with any local account including aliases (see Aliases), the SMTP Server will not relay for the user. If you check Verify sender by previous POP3 access, 602LAN SUITE's SMTP Server will only work for users who have already successfully accessed their POP3 mailboxes (using their login name and password). If you want to enable sending e-mail through 602LAN SUITE to ALL Internet user, uncheck both checkboxes.

SMTP relay
Relay for 602Pro LAN SUITE users only
Verify sender by previous POP3 access
IP filter defines access to SMTP relay
SMTP relay IP filter

WARNING! 602LAN SUITE's SMTP Server will be vulnerable to SPAM abuse if both checkboxes are unchecked! If you want to protect SMTP processing by the IP filter, check IP filter defines access to SMTP relay and setup the SMTP relay IP filter.

SMTP Relay IP Filter
The SMTP relay IP filter defines what connections are able to relay mail through the SMTP server. The IP filter rules are checked from top to bottom with each rule superceding those above it. Enter the IP address and mask of the computer or network that sends the request to the field IP address and IP mask. It is also necessary to define if the item is allowed or prohibited – RED means access denied, GREEN means permit access.



Web Mail

The Web Mail Client provides access to 602LAN SUITE mailboxes through an Internet Browser or wireless device that supports WAP (Wireless Access Protocol). All communication between the browser (client) and 602LAN SUITE (server) is running through the HTTP or HTTPS (Secure HTTP) protocol.

Login to the Web Mail client

Run an Internet browser and enter the IP address or domain of the computer where 602LAN SUITE is running (i.e. http://192.168.1.1/mail or http://www.yourdomain.com/mail):

- Enter your **Username** – This field is not case sensitive.
- Enter your **Password** – This field is not case sensitive.
- Click the **Login** button.

NOTE: If you are inactive for more than 60 minutes, the Web Mail Client will automatically log you out.

602LAN SUITE Web Mail Client Window

The main Web Mail Client window consists of two horizontal sections – the menu bar and the window according to the selected function. You can choose from the following functions:

- New message
- Mail
- Address Book
- Options
- Help
- Logout

The Help button displays the help page.
The Logout button will log you out from the server.

Mail

Each user account includes six folders:
Inbox, Drafts, Items to be sent, Sent items, List of sent items and Deleted items.
The left part of the window shows the folder tree and the right part shows the messages in the selected folder. The first folder in the folder tree is the Inbox.

Inbox

The Inbox is the default folder for delivered messages. You can create your own personal folders by entering a name for the new folder into the Create folder edit field and clicking the confirm button. Each

message includes a checkbox that allows you to select the message(s) for further processing (Delete, classify as Junk/Not Junk mail, Move or Copy to a folder).
The first checkbox above all the checkboxes is the Check all checkbox. By clicking this checkbox all checkboxes underneath will be checked automatically.

Each message has three attributes:

- Date and Time
- Sender
- Subject

NOTE: It is possible to sort messages by any one of these attributes.

To open a message, click the link of the message. The link will be placed on the sorting attribute.
The **Refresh** button updates the current folder message list. The actual list of messages will be read from 602LAN SUITE. This process is not automatic.
If you have many messages in a folder you can page through the messages via the two arrow buttons at the bottom. Between these arrows is the actual position indicator.

Drafts
The Drafts folder includes the list of messages that are not finished and you have saved for future editing.

Items to be sent
This folder includes the list of messages that are waiting to be sent. It is possible to proof a message that is waiting to be sent. Check on the checkbox of the message you want to proof and click the Disable button. Then click on the message link (according to the attribute that it is sorted by). The message will open and you can edit it. When you are done proofing, click the Close button. If satisfied, Enable the message to be sent. If you are not satisfied, you can delete it.
NOTE: It is not possible to edit a messages once in the Sent items folder.

Sent items
Each sent message will be copied into this folder. By default this option is disabled.
To enable this option check Save copy of every sent message to the Sent items folder checkbox in the Options menu.

List of sent items
This folder includes a list of sent messages. This is a log view only, message content can not be viewed.

Deleted items
If you delete a message from a folder, the message is firstly moved into the Deleted items folder.
To delete a message permanently you must delete it from this folder. To restore a message click the Restore button and the message will be restored.
It is possible to set an automatic deletion interval for this folder. If you want to delete messages from this folder automatically, enter the number of days into Delete messages after xxx days and click the confirm button.
To change the deletion interval, it is necessary to Disable automatic message deletion, then re-enter a new value (in days) for automatic message deletion.

New Message
A New Message includes the following fields:

- **From:** – If you do not have any aliases, only one address will be displayed. Otherwise you can select one of your aliases.
- **To:** – Click this link to select recipients. The Address Book window will open.
- **Carbon Copy (CC:)** – Click this link to select recipients. The Address Book window will open.
- **Attachments:** – Window to attach files will open.

- **Subject:** – Field to enter the identification string of the message. This string will be displayed in the recipient's list of messages.
- **E-mail edit field** – Textbox to write the message
- **Text Signature** – Check this if you want to add a text signature defined in the Options window.
- **Blind copies** – If you enter more then one recipient, it doesn't matter if in the To: or CC: field, and you check this checkbox, the header of the message will not include other recipients (each recipient will not know about the other recipients).
- **Request read receipt** – The message will be sent as registered. That means the recipient will have to confirm an open message dialog and you will receive a confirmation e-mail informing that the recipient has opened your message. 602LAN SUITE automatically generates this confirmation message.
- **Format** – Message format. Select the one you want according to the appropriate standard: MIME, RFC822 or UUEncode.

Spell Check
The Spell Check feature supports the American and British language. When you are done with a message you can proof it by spell checking. Click the SpellCheck button. A blue-framed field including the message text will appear. Incorrect words are in red. It is possible to correct them by typing new text into the Enter new spelling field or select a suggestion from the Suggestions field.

- **Ignore button** – Single (red) word will be ignored in this message
- **Ignore All button** – All word forms of the marked word will be ignored in this message
- **Add to Dictionary** – Word forms of the marked word will be added to the user's personal dictionary. This word form will not be marked as wrong in the following messages. User personal dictionaries are stored in the proper user mailboxes.
- **Change** – Single (red) word form will be changed in this message
- **Change All** – All word forms of the marked word will be changed in this message
- **Close** – Finish spell checking.

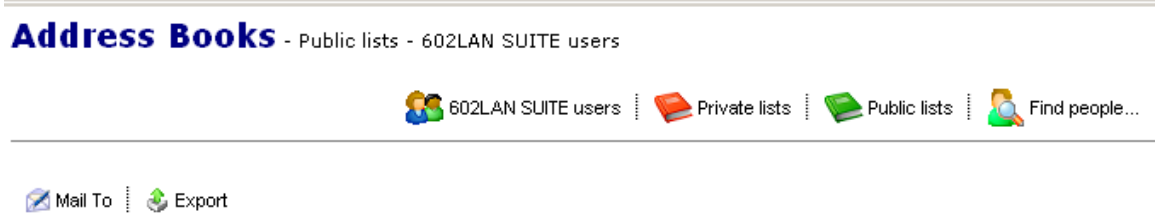
Send
To send the message, click the Send button.

Save Draft
If, for any reason, you can not finish the message, click the Save Draft button to save this message for future editing. The message will be saved into the **Drafts** folder.

Cancel
To cancel message composition, click the Cancel button.

Address Books
The **Address Books** window has three user lists:

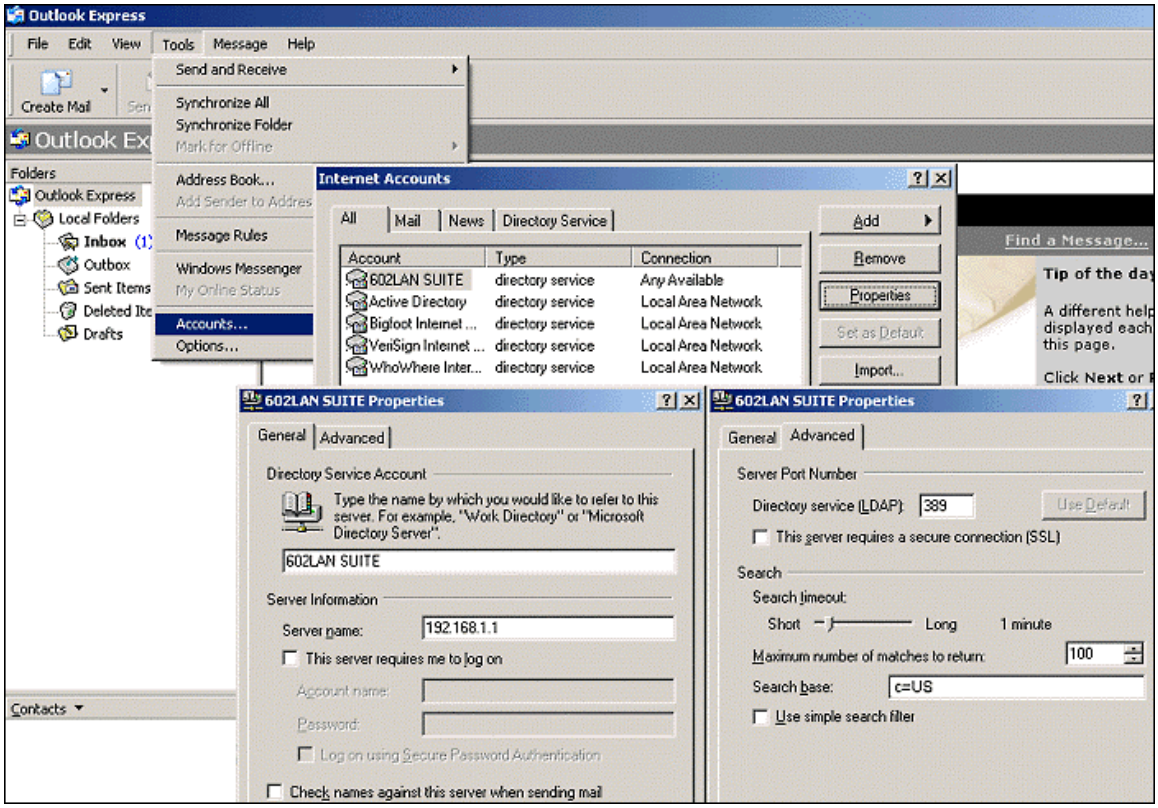
- **602LAN SUITE users** – This list includes all users who have an account on the 602LAN SUITE Server. It is possible to export the list of 602LAN SUITE users to a .CSV (comma delimited) file.
- **Private lists** – Each user can have his/her own private address list. It is possible to create as many private lists as needed as well as Import / Export users from / to a .CSV file.
- **Public lists** – Only users who have administrator rights can create / manage Public lists, as well as import users from a .CSV file.



Find people...
The 602LAN SUITE Find people tool uses a service known as Directory Services. The 602LAN SUITE Web Mail Client uses Directory Service accounts defined in Outlook Express located on the 602LAN SUITE server.

What are directory services?
A directory service is a powerful search tool that you can be used to find people and businesses around the world. The Address Book supports LDAP (Lightweight Directory Access Protocol) for accessing directory services, and it comes with built-in access to several popular directory services. You can also add additional directory services from your Internet service provider.
Like other Internet search tools, directory services use different methods for collecting data, so when you are trying to find a person or business online, you should try more than one service.

How to create a 602LAN SUITE Directory service
Run Outlook Express (located on the 602LAN SUITE server), click Tools / Accounts / Add / Directory service and fill it out according to the picture below.

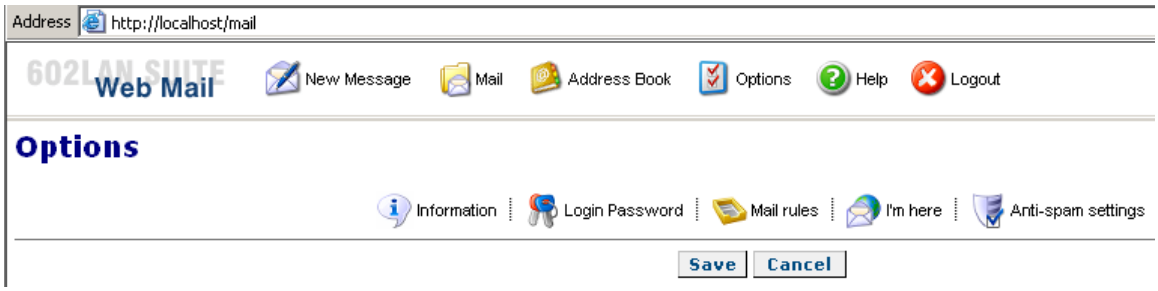


Most important is the Server name field on the General tab, it must include the IP address of the computer where 602LAN SUITE is running and the Search base on the Advanced tab must be the same as on the 602LAN SUITE server (Advanced Configuration - Users - LDAP directory). Please ask your administrator for assistance.
After Outlook Express is configured, click the Find people... button, select 602LAN SUITE in the Look in: field. To find an e-mail address defined in 602LAN SUITE enter a name or part of a name (e.g. bob), click the Find button and the 602LAN SUITE Directory service should return Bob's e-mail address.

Options
On top of the Options window are five buttons:

- **Information** – Displays the user information page

- **Login Password** – Here you can change your password
- **Mail Rules** – Here you can enter rules for incoming messages.
- **I'm away/I'm here** – If you are using Mail Rules, this button activates/deactivates rule processing based on the I'm away/I'm here status.
- **Anti-spam settings** - Here you can enter rules for junk e-mail processing.



Options menu

Layout

- **Show Inbox time** - Enable / disable the time panel on the Inbox page.
- **Line Width** - Maximum number of characters on a single line.
- **Preview first three lines of unread messages** - Enable / disable the three line message preview.
- **Messages per Page** - Number of messages to display in a folder at one time.
- **Highlight links to documents on Internet (URLs)** - If you check this checkbox, all text in your incoming messages that is recognized as links to Internet sites will be displayed as Internet links. You can click on them and the proper site will open in a new window.
- **Message Header** - Each Internet message includes a header. You can choose from three header modes: full header, no header or short header.
- **Enable folder tree** - Enables the folder tree in the Inbox.

Mail

- **Text signature** - Text signature to automatically add to the end of each e-mail you send.
- **Internet Message Format** - Internet message format
- **Default Address Book** - Select the default Address Book that will be displayed when you click To: or CC: during the creation of a new message.
- **Language for spell checking** - Select the default language for the spell checker.

Mailbox

- Save a copy of every sent message to the **Sent Items** folder.
- Move deleted messages to the **Deleted Items** folder.

Anti-virus support

Anti-virus support consists of two options:

- **Scan attached files of the new message** - Each attached file to a new message will be scanned for viruses.
- **Scan attached files of the opened message** - Each attached file to a received message will be scanned for viruses (upon opening the message).

Mail Rules

The Mail Rules window consist of two main parts:

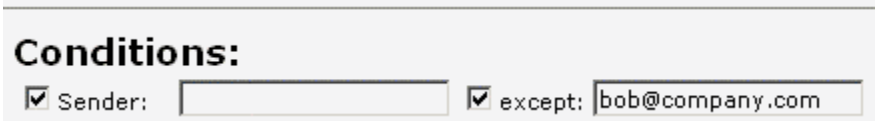
- Mail Rules will be processed based on conditions
- An Action will occur if the condition is satisfied

To add a new mail rule click Add new mail rule.

Process
Choose when the rule will be processed:

- **Always**
- **Only when I'm away** – See button on the Options window
- **Only when I'm here** – See button on the Options window
- **Never**

Conditions
Here you can set restrictions on the conditions. If you leave all conditions unchecked, ALL incoming messages will be processed according to the Process settings.
Example 1: This condition setting means that the rule will be used for all incoming messages except messages from bob@company.com



Example 2: This condition setting means that the rule will be used only for incoming messages from george@company.com

Action
If an incoming message complies with the Process and Conditions settings the defined action occurs. There are four actions:

- **Nothing** – Together with Delete when action finished you can set a rule for deleting specific messages.
- **Move to folder** – If you have your own folder(s) created (in the Inbox window), you can move incoming message to the selected folder.
- **Forward** – You can forward incoming messages to another e-mail address.
- **Reply** – You can automatically reply to incoming messages. It is not possible to reply to a fax.
- **Notify** – You can send a notification about an incoming message to another e-mail address. If the e-mail address is assigned to a cellular phone, it is possible to notify yourself about important incoming message. **Date and time**, **Sender Subject**, **Files count/size** and **Beginning of message text** checkboxes define parts of the incoming message that will be included in the notification message. **Max number of characters** - If you need to limit the size of the notification message (e.g. in the case you send it to a cellular phone with a limited display), enter the maximum number of characters of the message.

Notes

- It is NOT possible to enter more than one address into Sender, Recipient (Conditions part) and To, CC (Action / Forward part) fields. If you need it, create another rule.
- If you have defined more than one rule, rules will be processed from top to bottom.
- If you need to stop processing when a rule is completed, check the **Stop processing** button.
- If you need to temporarily disable a rule, create a rule with the Nothing action, check the **Stop processing** button and move the rule above the rules you need to disable.

© 2004 Software602, Inc. 9/2004

Anti-Spam Settings

What does SPAM mean?
SPAM is unsolicited junk e-mail sent to a large number of people to promote products or services.

Options

Checking methods

- **Use Whitelist and Blacklist to check incoming messages** - Enables the functionality of the Whitelist (Always receive e-mail from list) and Blacklist (Always reject e-mail from list).
- **Automatically add senders of messages classified by you to Whitelist or Blacklist** - If you classify a message as Junk / Not Junk by clicking the Junk / Not Junk icon, the sender of this message will be Automatically added to the Blacklist / Whitelist.

Message tagging
Incoming Junk e-mail will be tagged in the following ways:

- **Add the following subject text to message** - Enter text that will be added to the message subject and select the tag position (the beginning or end of the subject).
- **Add X-LNS-Spam-Check header to message** - Adds detailed information about this Junk message to the header.

Junk E-mail action
If an incoming e-mail is Junk e-mail, the web mail client provides the following actions:

- **Move to folder xxx** - Select the folder that the Junk e-mail will be moved to. The default folder is the Inbox.
- **Move to folder xxx created under xxx** - Enter the folder name for your Junk e-mail that will be created under the folder selected in the create under box.
- **Delete** - Incoming Junk e-mail will be automatically deleted.

Whitelist and Blacklist
602LAN SUITE provides two control lists:

- **Whitelist** - Messages from these senders will NEVER be classified as Junk E-mail.
- **Blacklist** - Messages from these senders are Junk E-mail.

You can Add, Edit or Delete any item in the list. You can also Import a list of e-mail addresses from a .CSV (comma delimited) file.

Automatic addition to the Whitelist
These two checkboxes enables/disables automatic addition of e-mail addresses to the Whitelist:

- **Add recipients of your sent messages** - It should be assumed that a recipient to which you send an e-mail to is someone you always want to receive e-mail from. So, by enabling this checkbox the recipient will automatically be added to your Whitelist.
- **Add other recipients of your received Not Junk messages** - If you classify a message as Not Junk, all recipients (in the TO or CC field) of this message will be automatically added to your Whitelist. You do not want to reject messages from all recipients of a message you classified as Not Junk.

WAP Access

602LAN SUITE also provides access to mobile wireless devices via WAP (Wireless Access Protocol). Most Internet capable cellular phones and some PDA devices support this protocol.

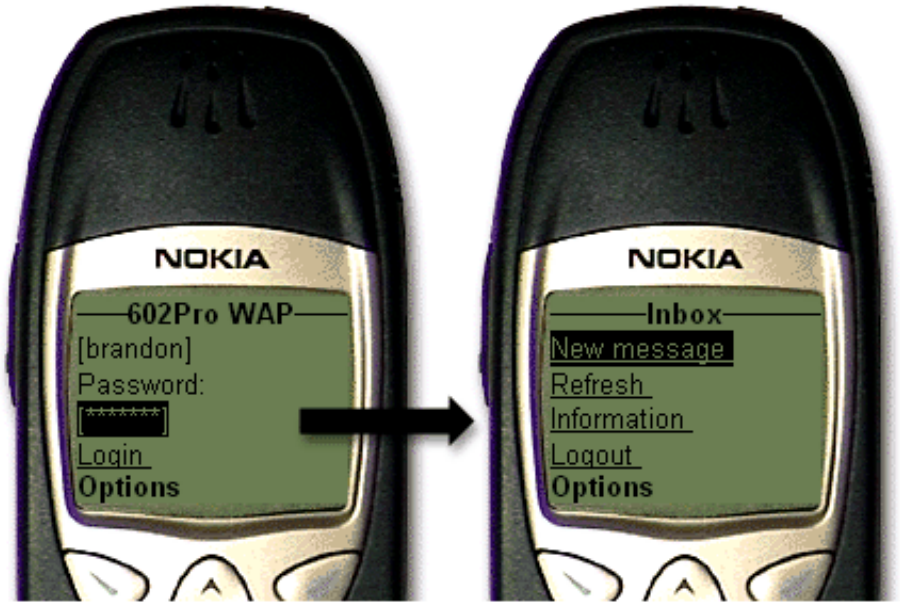
Requirements

- Internet capable phone that supports WAP (wireless access protocol) most "Internet Capable" wireless phones meet this requirement.
- Internet Access service for your phone.
- An Internet connection for 602LAN SUITE that either has a static IP address, domain name or dynamic DNS service.

Setup

Due to the differences in each phone setup we cannot offer specific instructions on how to configure individual phones. Please use the following steps as a reference guide instead of exact instructions. For assistance, please consult your phone's user manual or manufacturer. Additional information about WAP is available at http://www.yourwap.com/.

1. On your phone, go to your favorite places.
2. Add a new favorite place and give it a name like "EMAIL".
3. For the URL, enter the web address of your 602LAN SUITE server and add /WAP on the end. If you are using an Internet connection with a static IP address, your URL would look something like this: http://206.182.14.251/wap or http://www.yourdomain.com/wap
4. Save your new favorite place.



Anti-Spam Protection

602LAN SUITE provides Anti-spam protection in four ways:
602LAN SUITE SMTP server immediately rejects / never rejects incoming message:

- **DNSBL services** – 602LAN SUITE can rejects messages according to the outcome of a request sent to a DNS lookup service.
- **SMTP Server Blacklist and Whitelist** – 602LAN SUITE can reject messages from hosts/senders entered into the blacklist. Messages from hosts/senders entered into the whitelist will never be rejected. This is a global list common for all 602LAN SUITE users.

Incoming messages will always be accepted. They will be tagged with message subject / header text and processed according to the settings:

- **Bayesian filter** – Bayesian spam filtering is an advanced content classification filter. 602LAN SUITE can recognize junk e-mail and perform a chosen action on the basis of previously classified Junk and Not Junk messages.
- **Personal Blacklist and Whitelist** – These lists are personal user lists manageable from the 602LAN SUITE Web Mail Client. Each user has his/her own personal blacklist and whitelist.

Protection via DNS Blacklist (DNS-BL)

602LAN SUITE will immediately reject incoming messages according to the outcome of a request sent to a DNS lookup service. Protection via DNS Blacklist (DNS-bl) is a cooperative effort by providers across the Internet to deny service to known spam domains. Some provide this service for free (in 602LAN SUITE the Anti-spam list includes the keyword [FREE]) and some of them not (keyword [PAY]). There are many anti-spam database categories:

- **Spam** – Includes confirmed spammers. Highly recommended.
- **Dial-up** – Includes dynamic assigning IP addresses. Recommended.
- **Open Relays** – Includes unsecured e-mail servers on the Internet that will relay e-mail for anyone. Highly recommended.
- **Combined** – Includes any combination of the above. Use at your own discretion.
- Add a service by clicking the Add button. To edit a service, click the Edit button:
- **Service name** – Descriptive name of a DNS lookup anti-spam service provider.
- **DNS lookup domain** – The lookup domain on which the service runs.
- **IP address returned when host is listed** – The anti-spam service provider defines the returning IP address if the domain from which the e-mail is coming is in the spam database.
- **Response if denied** – Define the text message to send if the incoming e-mail is from a spam domain.

To delete a service, click the Delete button.

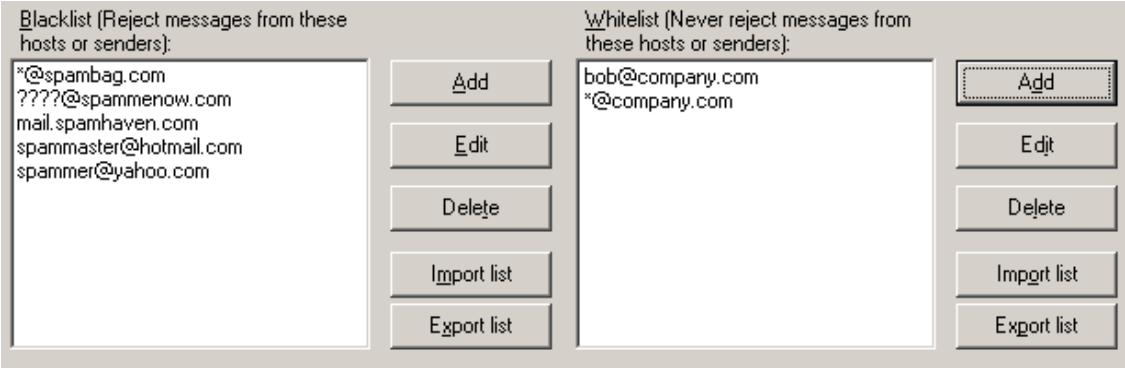
SMTP Anti-spam settings
Use selected ip4r (DNSBL-style) DNS lookup services to reject messages from spam hosts:
Blackholes at five-ten-sg.com (Spam) [FREE] - http://www.five-ten-sg.com/blackhole.php
Blackholes at five-ten-sg.com (Dial-up) [FREE] - http://www.five-ten-sg.com/blackhole.php
Blackholes at five-ten-sg.com (Unconfirmed opt-in) [FREE] - http://www.five-ten-sg.com/blackhole
easynet.nl Blackholes (Spam) [FREE] - http://abuse.easynet.nl/blackholes.html
Open Relay Database (Open Relays) [FREE] - http://www.ordb.org/
NJABL.ORG (Open Relays) [FREE] - http://njabl.org/
NJABL.ORG (Dial-up) [FREE] - http://njabl.org/
NJABL.ORG (Spam) [FREE] - http://njabl.org/
MAPS RBL+ (Combined) [PAY] - http://mail-abuse.org/rbl+/
Add service
Edit service
Delete service

Protection via the SMTP Blacklist and Whitelist

If you need to define the SMTP server Blacklist and Whitelist, click the SMTP tab then SMTP Anti-spam settings button. 602LAN SUITE SMTP server immediately rejects / never rejects incoming message according to these lists.

Here you can enter a specific sender or host from which you do not want to accept e-mail from (Blacklist) OR from which you always want to accept e-mail from (Whitelist). It is possible to edit or delete a single item. Specific senders or hosts can be imported/exported from/to a file. The format of the file must be a plain text file with only one sender/host per line.

- **Host** - A host would be the mail host of the sender. If the mail host for e-mail address bob@company.com is mail.company.com enter mail.company.com.
- **Sender** - The sender would be the complete e-mail address of the sender. To block/ allow bob@yahoo.com, enter bob@yahoo.com. To block/allow ALL addresses from company.com enter *@company.com.



NOTE: A host can send e-mail for multiple domains. So, you could possibly be blocking mail from more than one domain.

Protection via Bayesian filter

What does SPAM mean?
SPAM is unsolicited junk e-mail sent to a large numbers of people to promote products or services.

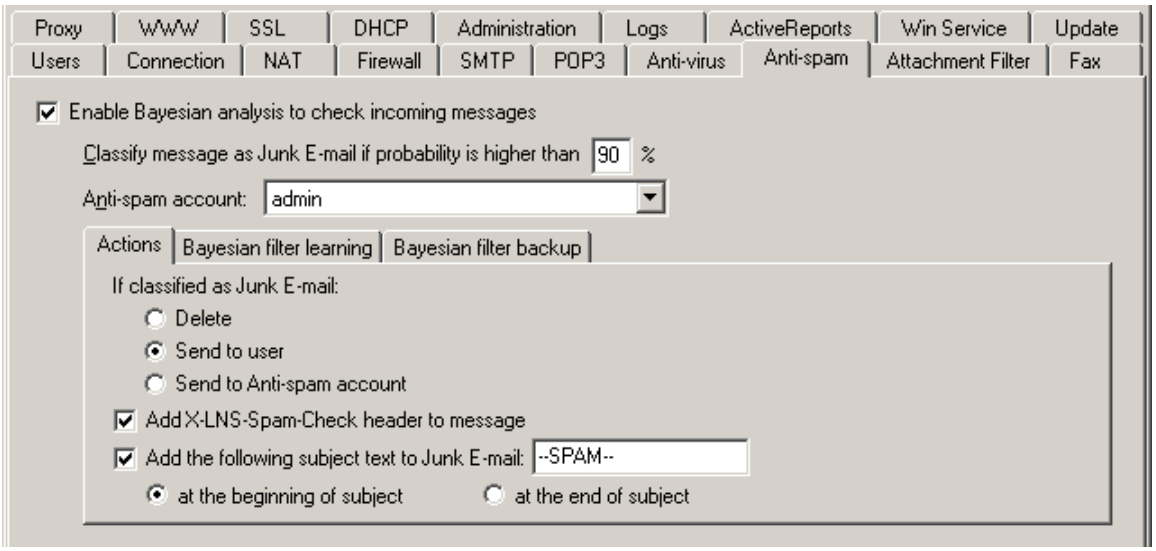
Technical Bayesian filter description: http://spambayes.sourceforge.net/.

Architecture
The architecture of the Bayesian system has a few distinct parts. The first, and most obvious, is the content engine that takes an e-mail message and breaks it up into a series of words. At this moment it takes words out of the text part of the message, stripping out various HTML code and other bits of unneeded information (e.g. images). A variety of e-mail header interpretation and internal serialization goes on as well.

Junk and Not Junk E-mail
The Bayesian filter will attempt to classify incoming e-mail messages as Junk or Not Junk (good e-mail). This means you can have Junk messages automatically filed away into a different e-mail folder where it will not interrupt your e-mail reading.

At first, the Bayesian filter must be trained to identify Junk and Not Junk e-mail. Essentially, you will show the Bayesian filter a number of e-mail that you like (Not Junk) and a number of e-mail you do not like (Junk). The Bayesian filter will then analyze the e-mail for clues as to what makes the messages different. For example: different words, differences in the e-mail headers and content style. The system will then use these clues to examine new incoming e-mail messages.

The 602LAN SUITE Bayesian filter
The 602LAN SUITE Bayesian filter will classify incoming e-mail messages and the outcome of this classification will be entered into the e-mail header. If incoming e-mail is classified as Junk, 602LAN SUITE can (according to the settings) insert a text string into the e-mail subject and insert a score into the e-mail header.



How to train the 602LAN SUITE Bayesian filter
Users can train the Bayesian filter in several ways:

- Web Mail – Users can classify received e-mail by clicking the Junk or Not Junk icons in the inbox.
- Any POP3 client – Users can classify received e-mail by forwarding the e-mail to the correct e-mail address: junk@junk for Junk or notjunk@junk for Not Junk.
- Personal Whitelist – It is possible to check the option **Automatically learn from senders listed in the white list** checkbox on the Bayesian filter learning tab and these messages will train the Bayesian filter automatically.

Bayesian filter Actions
If the 602LAN SUITE Bayesian filter classifies incoming e-mail as Junk mail, it is possible to select one of three actions:

- **Delete** – Deletes the message immediately
- **Send to user** – Send the message to the user
- **Send to Anti-spam account** – Send the message to the Anti-spam account for further processing

You can define the following options regardless of action:

- Add X-LNS Spam-Check header to the message
- Add the following subject text to Junk E-mail

Bayesian filter training

- Check the Automatically learn from senders listed in the white list checkbox. The 602LAN SUITE Bayesian filter will use messages from these senders to train itself automatically.
- Select a method on how the Bayesian filter will be updated when users classify e-mail as Junk or Not Junk.

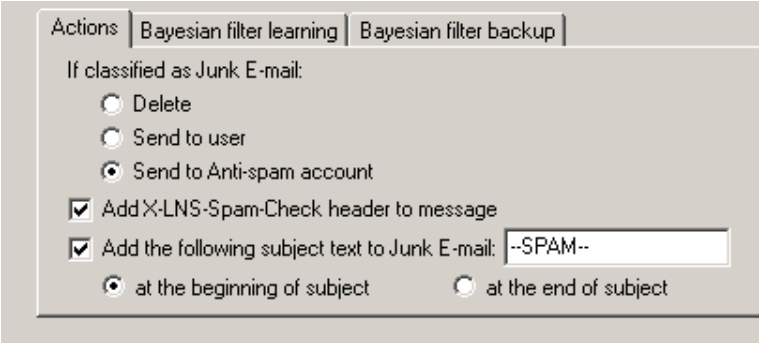
Bayesian filter backup
The 602LAN SUITE Bayesian filter database can be saved at anytime. We recommend backing up the database to repair a situation when a large amount of messages has been improperly trained. In this case you can restore a previous Bayesian filter database.

© 2004 Software602, Inc. 9/2004

602LAN SUITE Anti-spam account
The Anti-spam account can be assigned to any 602LAN SUITE user, but we recommend creating a dedicated user account for junk e-mail.

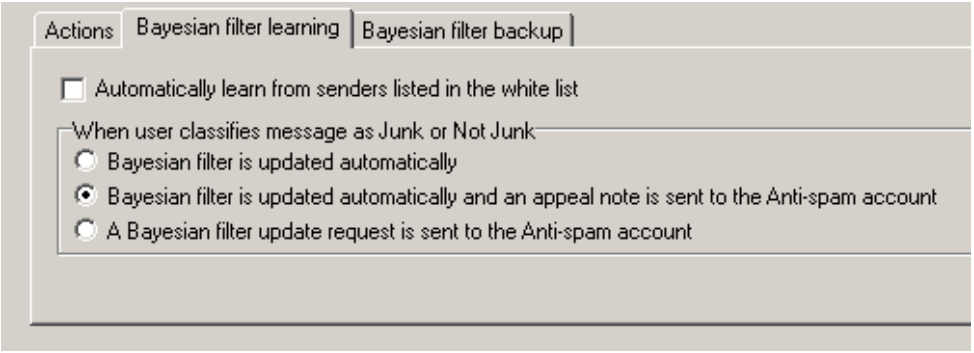
How does the Anti-spam account work?

- Messages classified as junk e-mail will be delivered to this account.



The Administrator or anyone who knows the login name and password to this account can periodically check e-mail here for improperly classified Junk e-mail (false positives).

- According to the Bayesian filter learning settings, a message is sent to this account informing that the Bayesian filter was updated **OR** an update request will be sent.


Actions
Bayesian filter learning
Bayesian filter backup
Automatically learn from senders listed in the white list
When user classifies message as Junk or Not Junk
Bayesian filter is updated automatically
Bayesian filter is updated automatically and an appeal note is sent to the Anti-spam account
A Bayesian filter update request is sent to the Anti-spam account

Protection via the Personal Blacklist and Whitelist

Each user has their own personal Blacklist and Whitelist. To define personal Blacklist and Whitelist, run the 602LAN SUITE Web Mail client, click Options then the Anti-spam settings button.

Here you can enter a specific sender or host from which you do not want to accept e-mail from (Blacklist) OR from which you always want to accept e-mail from (Whitelist). It is possible to edit or delete a single item. Specific senders or hosts can be imported/exported from/to a file. The format of the file must be a plain text file with only one sender/host per line.

- **Host** - A host would be the mail host of the sender. If the mail host for e-mail address bob@company.com is mail.company.com enter mail.company.com.
- **Sender** - The sender would be the complete e-mail address of the sender. To block/allow bob@yahoo.com, enter bob@yahoo.com. To block/allow ALL addresses from company.com enter *@company.com.

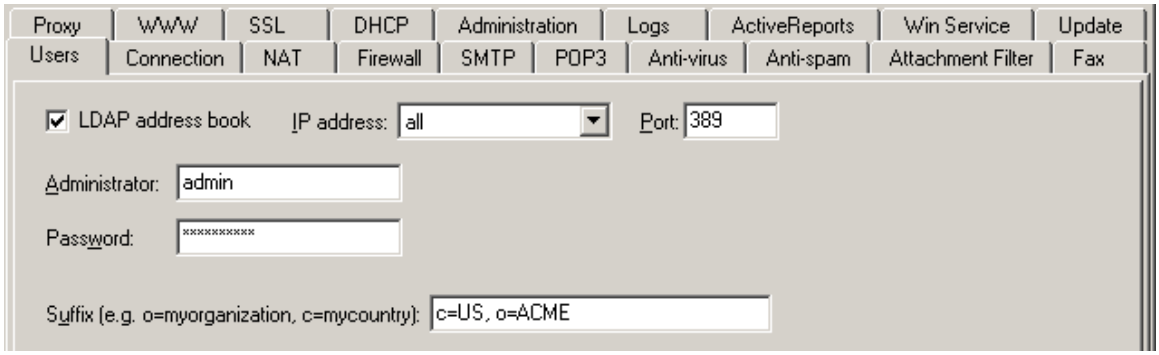
NOTE: A host can send e-mail for multiple domains. So, you could possibly block mail from more than one domain.

LDAP Address Book Setup

LDAP

To begin using the LDAP Address Book in 602LAN SUITE you must first check the box in the upper left-hand corner of the LDAP tab.

- **IP address -** If the computer where 602LAN SUITE is running works as a gateway to the Internet and has two network adapters, you have several choices.
  - **Select the IP address of the INTERNAL network** – User information will be opened to the internal network only.
  - **Select the IP address of the EXTERNAL network** – User information will be opened to the external network only (to the Internet but NOT your LAN).
  - **Select all interfaces** – User information will be opened to the Internet as well as to your LAN.
- **Port Selection:** The default port LDAP listens on is 389. If you change the value, all clients will have to change the LDAP port configuration as well.



Setting Up Microsoft® Outlook Express as an LDAP Client

If you are configuring Outlook Express to work as an LDAP client, do the following:

1. Click the Tools menu and select Address Book.
2. In the Address Book window select the Tools menu and select Accounts.
3. When the Internet Accounts window appears click the Add button to add a new directory.
4. For Internet directory (LDAP) server, type the hostname/IP address of your 602LAN SUITE server (probably 192.168.1.1), then click Next.
5. Select Yes and then click Next.
6. Click Finish.
7. The new directory name will appear in alphabetical order in the left column.
8. Select the Directory Service that you just entered and then click Properties.
9. Click the Advanced tab.
10. For search base enter c=US if that is what country suffix is entered on the LDAP tab in 602LAN SUITE. Now click OK.
11. Now, from the Address Book select Find People.
12. Under Look in select the directory you just added.
13. Click the Advanced tab
14. For Define Criteria select E-mail contains, enter an @ sign, then click Add.
15. Finally, click Find Now to display a list of all users in the 602LAN SUITE user list.

Practical Use for LDAP

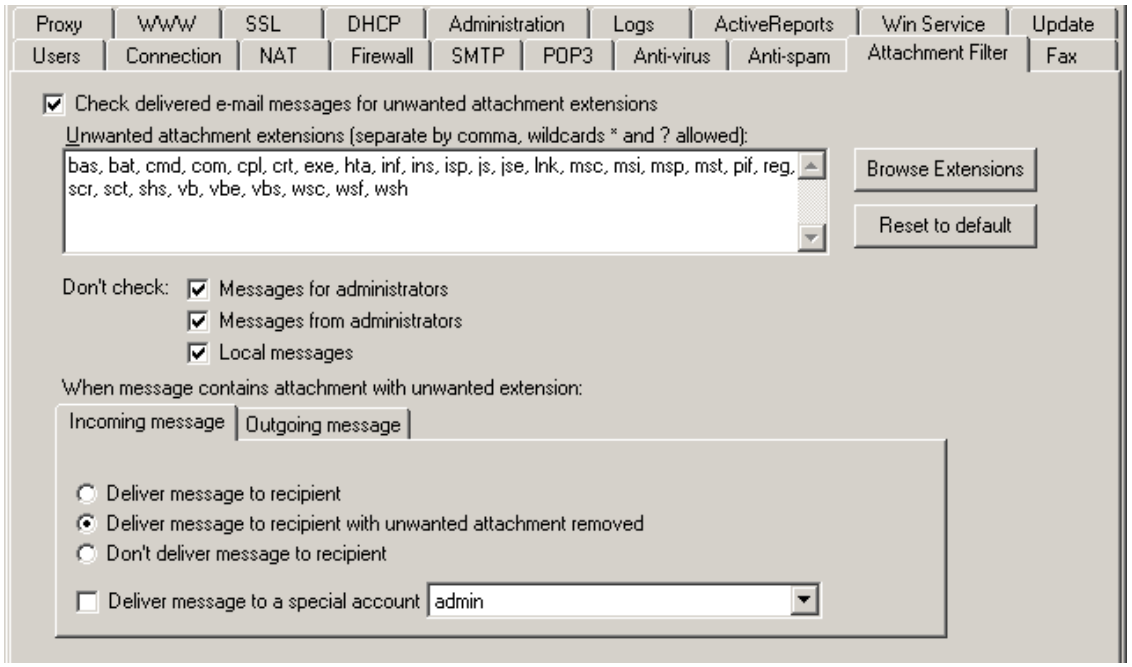
Users using an e-mail client that includes an LDAP Client (i.e. Outlook Express) can import addresses from the LDAP Directory. The LDAP Client will connect to 602LAN SUITE's LDAP Address Book and pick up all company e-mail addresses entered on the Users tab who have been provided the option to appear in the LDAP directory.

© 2004 Software602, Inc. 9/2004

Attachment Filter

Incoming/outgoing messages can include attached files. It is possible to define file extensions for message attachments that will be checked by 602LAN SUITE on this tab. Messages including these attachment extensions will be processed according to the following settings:

- **Check delivered e-mail messages for unwanted attachment extensions** – Enable/Disable attachment filtering.
- **Unwanted attachment extensions** – Enter the extensions of attached files that will be processed by the attachment filter.
- **Don't check** – Choose if you want to check messages for/from Administrators or local messages.
- **Incoming/Outgoing message** – Here you can define an action if a message includes an unwanted attachment extension.

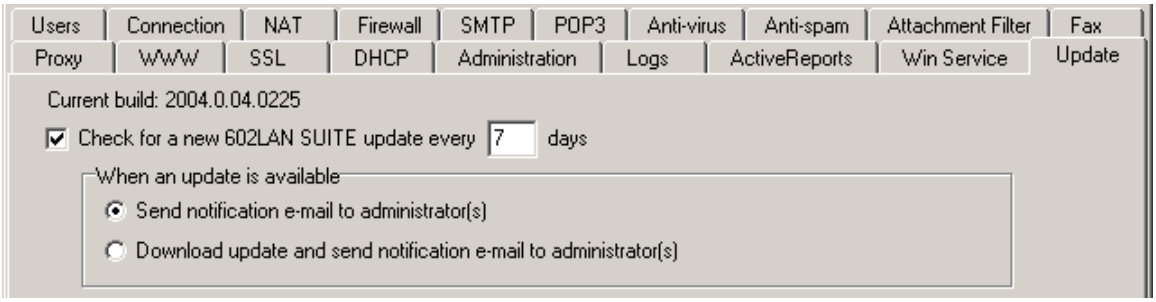


Update Manager

602LAN SUITE can automatically check the Software602 Update Server for new updates. If you want 602LAN SUITE to check for new updates automatically enable the Check for a new 602LAN SUITE update every xxx days checkbox.

When a 602LAN SUITE update is available, one of the following options determine the result:

- **Send notification e-mail to administrator(s)** – An update notification will be sent to all administrators.
- **Download update and send notification e-mail to administrator(s)** – The new update will be downloaded and an update notification will be sent to all administrators.



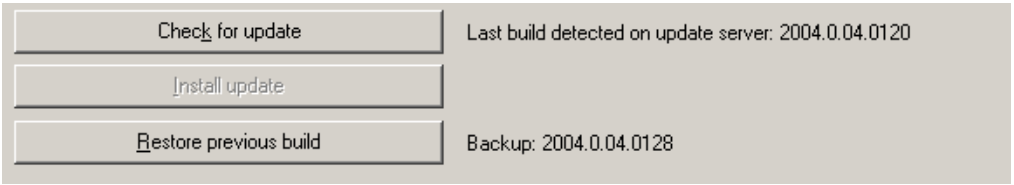
If you want to limit the time in which the update will be downloaded, check the Limit update time from checkbox and enter the required time values. The default time interval is 00:00 – 5.00AM.

If 602LAN SUITE is connected via a Dial-up Internet connection and you want to automatically establish a Dial-up connection to download the update, check the Establish dial-up connection to download update checkbox.

If necessary, fill out the HTTP proxy address if you need to use an HTTP proxy server to connect to the update server.

Limit update time from 00:00 to 05:00
Establish dial-up connection to download update
Use HTTP proxy to communicate with update server:

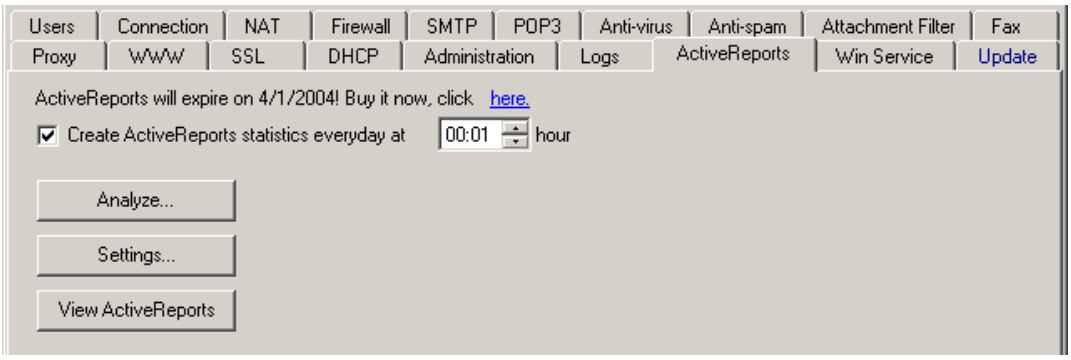
If you do not want to use the automatic option, you can still check the update server for new 602LAN SUITE update manually by clicking the Check for update and Install update buttons.



The previous build of 602LAN SUITE will be automatically saved. If any error occurs during startup of the new build of 602LAN SUITE, the previous build will be restored.

ActiveReports

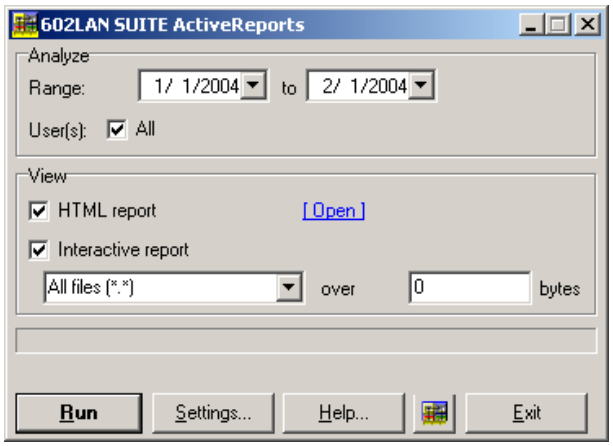
ActiveReports is a 602LAN SUITE plug-in that is designed to read and analyze 602LAN SUITE log files. ActiveReports creates individual statistic HTML pages for each LAN workstation as well as for the entire LAN. Total data size usage is displayed in charts for years, months or days. You can also see total values or filter results according to certain protocols (HTTP, SOCKS, etc.). Check Create ActiveReports statistics everyday at xxx hour and ActiveReports will run daily at this preset time. It is also possible to start analysis manually by clicking Analyze... on this tab. For more information see ActiveReports help.



ActiveReports will run in Trial mode for 30 days with full functionality. To continue using the application after this period, it is necessary to purchase ActiveReports.

How it Works

ActiveReports will run daily at the preset time defined in 602LAN SUITE and analyze the log file from the previous day. When analysis is finished, ActiveReports will create individual statistic HTML pages for each LAN workstation. These HTML statistics are available at **http://www.yourdomain.com/stat/**. The appropriate statistics will be displayed according to the host from where the request comes.



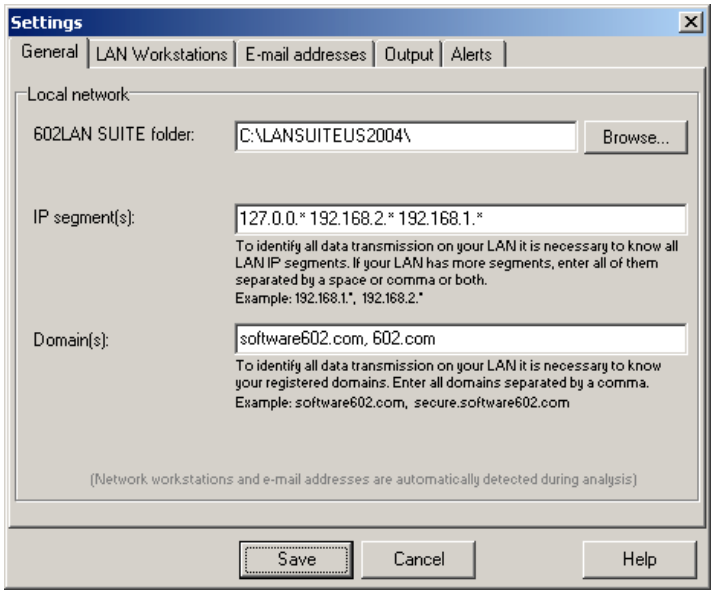
Statistics for the entire LAN are available at **http://www.yourdomain.com/admin/stat/**. This will require a login from an administrator. Transmitted data size is displayed in visual charts by years, months or days. You can see results as total values and it is possible to filter results according to a specific protocol (HTTP, SOCKS, etc.).

For more detailed information (to see downloaded files, sent/received messages, etc.) run ActiveReports in interactive mode (602LAN SUITE - Statistics - 602LAN SUITE ActiveReports - Analyze...) with the required date range. ActiveReports shows workstation totals by transmitted data sizes for the selected amount of days by the selected protocol, list of HTTP requests or list of received/sent messages. It is also possible to save the charts as well as the lists of files (charts to .BMP/.GIF and lists to .CSV).

Settings

General tab

- **602LAN SUITE folder** - Enter the folder where 602LAN SUITE is installed. This folder includes the .LOG files that ActiveReports will analyze.
- **IP Segment(s)** - LAN workstation IP addresses are usually 192.168.1.x where x is an interval from 1 to 254. If you use other IP addresses enter the '*' character instead of the number that is different from the number on the same position in the IP address. If your LAN has more than one segment, enter all of them separated by a space. If you leave this field empty, the 192.168.* and 10.* mask will be used for analysis.
- **Domain(s)** - To identify all data transmission on your LAN it is necessary to know your registered Internet domains. Enter all domains separated by a comma.


Settings
General
LAN Workstations
E-mail addresses
Output
Alerts
Local network
602LAN SUITE folder:
C:\LANSUITEUS2004\
Browse...
IP segment(s):
127.0.0.* 192.168.2.* 192.168.1.*
To identify all data transmission on your LAN it is necessary to know all LAN IP segments. If your LAN has more segments, enter all of them separated by a space or comma or both.
Example: 192.168.1.*, 192.168.2.*
Domain(s):
software602.com, 602.com
To identify all data transmission on your LAN it is necessary to know your registered domains. Enter all domains separated by a comma.
Example: software602.com, secure.software602.com
(Network workstations and e-mail addresses are automatically detected during analysis)
Save
Cancel
Help

LAN Workstations

The LAN Workstation list is the most important list in ActiveReports. All LAN activity is analyzed according to this list. LAN IP addresses are automatically detected (according to the entered IP segment(s)) during analysis. It is possible to assign user account(s) to IP addresses to ensure the correct assigning of user e-mail addresses to IP addresses. For a better description it is suggested to enter a full name for each account as well. To change the order of IP addresses within this list use the Up/Down buttons.

E-mail addresses

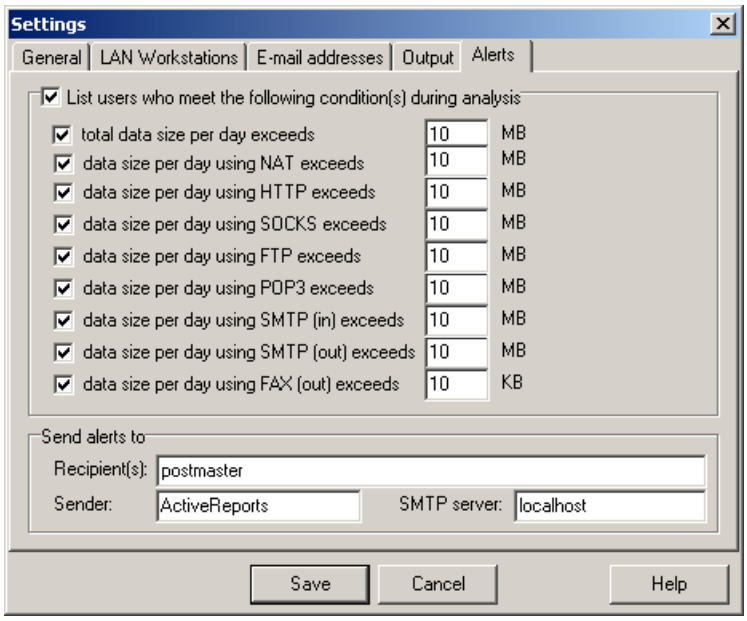
It is also necessary to assign e-mail addresses to the IP addresses found on the LAN Workstations tab. If an e-mail address is not from your LAN (e.g. when a user uses a free e-mail address as the sender e-mail address to send e-mail from your LAN) it will need to be manually entered here.

Output

- Destination folder - Statistic HTML pages will be saved into this folder. The default path is LANSUITE_FOLDER/ADMIN/STAT/
- User description - Select how users will be described in the HTML statistic pages.
- Generate month charts in days - Monthly charts will be generated and saved as days. This option takes longer to execute and occupies more disk space.
- List e-mail addresses - E-mail addresses assigned to users will be displayed on the HTML statistic pages concerning SMTP analysis.
- List domains and downloaded files - Visited domains and downloaded files will be displayed on the HTML statistic pages concerning HTTP requests.

- List number of dial-up attempts - Number of dial-up attempts (in addition to the dial-up connection time) will be displayed on the HTML statistic pages concerning dial-up analysis.
- Enable data size accuracy within xxx decimal places - Enter the number of decimal places for data size accuracy.

Alerts
When ActiveReports is running in automatic daily analysis mode it is possible to send e-mail alerts to designated e-mail addresses. To enable this feature check the top checkbox List users who meet the following condition(s) during analysis. Now select the conditions you want to be alerted on and enter the data size to trigger this alert. Finally, enter the e-mail address(es) to the Recipient(s) field and separate them with a semi-colon. Enter the sender e-mail address to the Sender field and your SMTP server IP address to the SMTP server field.


Settings
General
LAN Workstations
E-mail addresses
Output
Alerts
List users who meet the following condition(s) during analysis
total data size per day exceeds 10 MB
data size per day using NAT exceeds 10 MB
data size per day using HTTP exceeds 10 MB
data size per day using SOCKS exceeds 10 MB
data size per day using FTP exceeds 10 MB
data size per day using POP3 exceeds 10 MB
data size per day using SMTP (in) exceeds 10 MB
data size per day using SMTP (out) exceeds 10 MB
data size per day using FAX (out) exceeds 10 KB
Send alerts to
Recipient(s): postmaster
Sender: ActiveReports
SMTP server: localhost
Save
Cancel
Help

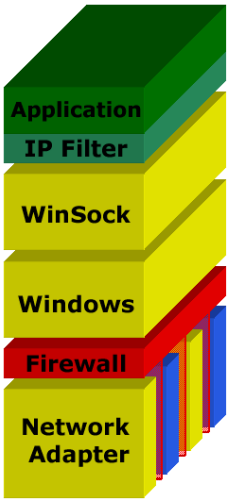
NOTE: ActiveReports can be started manually from the command prompt with the /SaveAll parameter to send alerts (e.g. c:\program files\software602\602lan suite\lstm.exe /saveall).

Advanced Access Control

Firewall

The firewall protects the computer where 602LAN SUITE is running and the entire Local Area Network against unauthorized TCP/IP connections. It is necessary to have at least two interfaces (1 - internal connection to your Local Area Network and 2 - External connection to the Internet). The firewall is available for the following operating systems:

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows XP Home
- Windows XP Professional
- Windows 2003 Server



First, the firewall security level must be set. You must select one of four options:

- High
- Medium
- Low
- Custom

NOTE: Improper firewall settings can cause disruption of 602LAN SUITE services such as SMTP, POP3, Proxy, WWW, etc. Read this chapter carefully!

WARNING: The firewall rules supercede the IP filter rules. This means that access to a given service that is denied by the firewall will never get to the IP filter!

For proper firewall functionality choose the interface to which your LAN is connected (your internal network interface). Interfaces not selected are designated as Internet interfaces.

If you do not check any interface as the internal network interface, only the computer where 602LAN SUITE is running will be protected. Remember each set or rule means ALLOW access. **If no rules are defined then ALL IP communication is denied!**

When creating a firewall rule set or adding a single rule it is necessary to understand TCP/IP connection principles. Here are the most important:

IP connection establishing and refusing

Source station (client station - source IP address:port) establishes the TCP connection and connects to the Destination station (server station - destination IP address:port).

Common applications always have the same port. In other words, you do not need to know in advance what port on a distant machine accepts e-mail, because every machine everywhere uses port 25 to accept e-mail. If an e-mail server is running on a machine and is ready to accept e-mail, the server application opens port 25 and listens for incoming e-mail. Here are some common ports:

- SMTP - port 25
- WWW - port 80
- POP3 - port 110
- LDAP - 389
- SSL - port 443

To view a complete list visit:

http://www.iana.org/assignments/port-numbers
Ports 0 through 1023 are reserved for common usage and are known as **Well Known Ports** (e.g. FTP port 21). Ports from 1024 through 49151are known as **Registered Ports** (e.g. IRC port 6667). **Dynamic/Private Ports** are those from 49152 through 65535.

You might think that the application sending e-mail uses port 25, but that is not the case. The usual procedure involves an application requesting and being given a socket by the operating system; that is, it asks for and receives a port. Any port will do (the application doesn't even need to know what the exact port number is), but the operating system will issue a port from somewhere above 1023. This port is used briefly, and then returned to the pool for another application to use later. The application sending the e-mail, using a port above 1023 sends a connection request to the standard port. When the connection is established, part of the information in each packet is the source IP address and port as well as the destination IP address and port. The port above 1023 is the source port; the standard port is the destination port. The destination machine will return packets using the original port above 1023 as its destination port. Although this sounds complicated, the underlying principle is easy to grasp: when a program uses a port above 1023, replies arrive back at that same port. Here's one last bit of complexity. Since standard listening ports are for everybody, the destination machine does not actually use it for data transfer. It only listens on that port. As soon as a connection is established it hands that connection to a local port above 1023 and immediately resumes listening for a new incoming connection request on the standard port. That is how a web server can listen for (and handle) thousands of connections from users.

Protocols
TCP (Transport Control Protocol) is known as a connection-oriented protocol, which means that a connection is established and maintained until the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

UDP (User Datagram Protocol) packets do not establish "permanent" connection. The sender sends out UDP packet and does not care about them anymore. To manage these connections it is necessary to set the allowed direction of a UDP connection. This means, to allow connections from your LAN to the Internet and their solicitation (e.g. A computer from your LAN send a DNS request to a DNS server located somewhere on the Internet and expects an answer. This is a solicited packet).

ICMP protocol (packets) is a service protocol. It signals various events in networks built on the IP protocol (Destination Unreachable, Redirect, Echo Request, Router Advertisement, Router Solicitation, etc.). The ICMP protocol is used in the PING and TRACERT commands. Destination Unreachable and Redirect messages are regarded as the most dangerous. If you want to allow basic diagnostics you can allow the following messages:

- Outgoing ICMP 8 (Echo Request)
- Incoming ICMP 0 (Echo reply - this message uses ping command)
- Incoming ICMP 11 (Time exceeded - uses Tracert command)

We recommend restricting other ICMP messages.

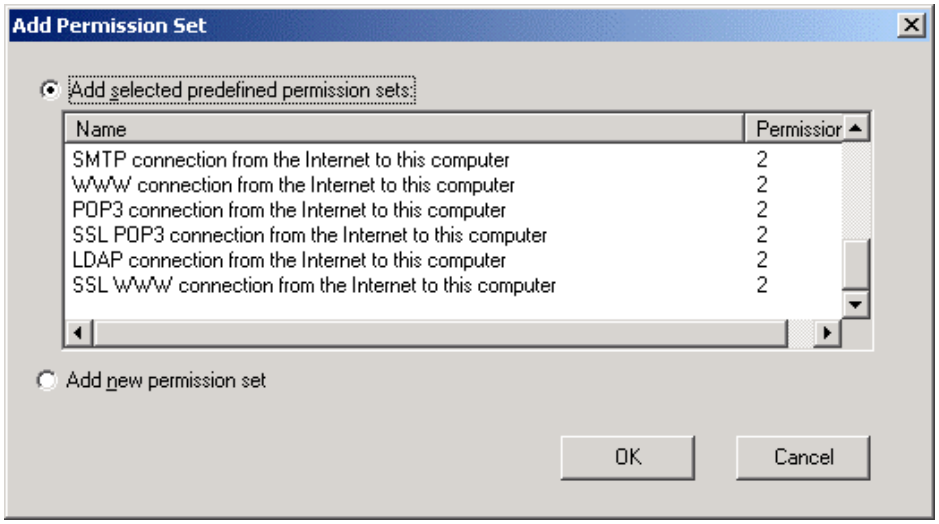
Firewall tab description
The computer where 602LAN SUITE is running must have at least **two interfaces:**

- **Internal** - NIC (Network Interface Card) connected to your Local Area Network (LAN)
- **External -** Analog modem, ISDN or second NIC connected to the Internet

To use the Firewall first check the **Firewall** checkbox in the upper-left corner of the Firewall tab. Then you must select your internal network interface(s). The firewall protects the computer where 602LAN SUITE is running plus your LAN connected to the internal network interface (filters TCP/IP packets).
Now you are ready to choose the security level. We recommend selecting one of the predefined security levels - **High**, **Medium** or **Low**. Once you select a security level, carefully read the description on the right-hand side.

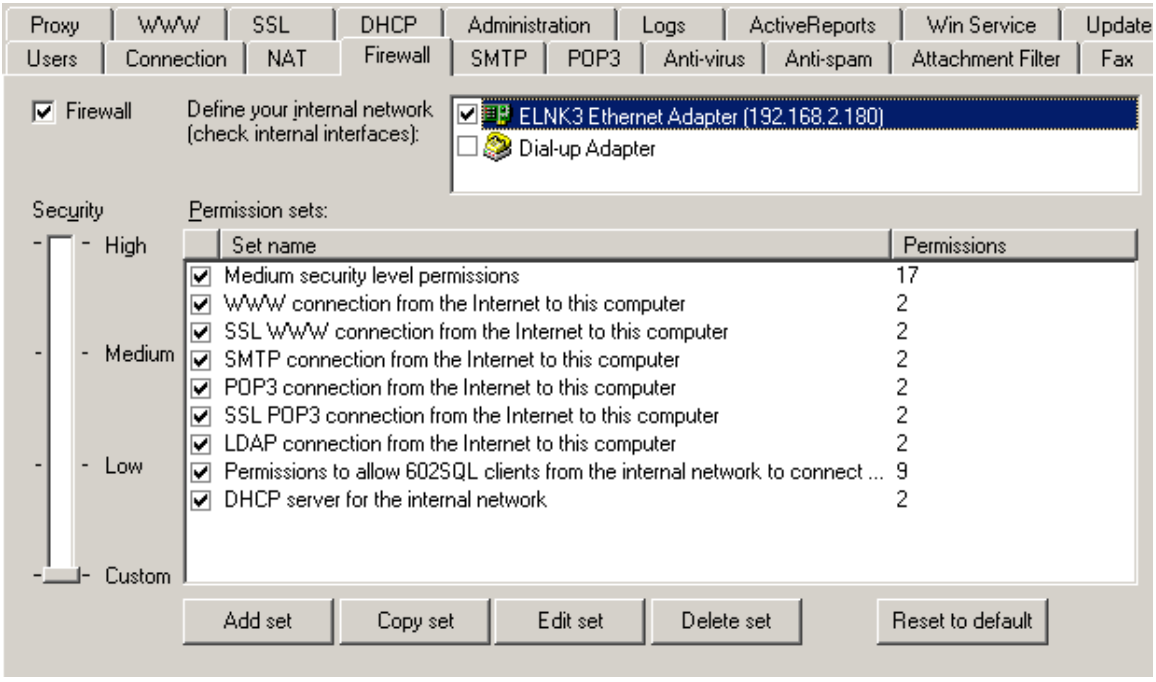
Using SMTP/POP3/WWW/LDAP servers with High or Medium security level

You should know that if you set the security level to High or Medium all TCP connections from the Internet will be denied including requests to 602LAN SUITE's SMTP, WWW, SSL WWW, POP3, SSL POP3 and LDAP servers. You can easily allow access by adding the proper predefined permission set.


Add Permission Set
Add selected predefined permission sets:
Name
Permissior
SMTP connection from the Internet to this computer 2
WWW connection from the Internet to this computer 2
POP3 connection from the Internet to this computer 2
SSL POP3 connection from the Internet to this computer 2
LDAP connection from the Internet to this computer 2
SSL WWW connection from the Internet to this computer 2
Add new permission set
OK
Cancel

Custom Security Level

If you select the **Custom** level all Firewall settings are under your control. You can add predefined security set(s), create new one(s), edit or delete them.



Adding a new set
Click the **Add set** button on the Firewall tab. The **Add Permission Set** window will appear. Here you can choose between two options:

- **Add selected predefined permission set** - Here you will find all predefined permission sets. You will also find the High, Medium and Low security level permissions here as well (you can modify the set but you must save the set under a different name).
- **Add new permission set** - Select this option if you want to create a new custom permission set.

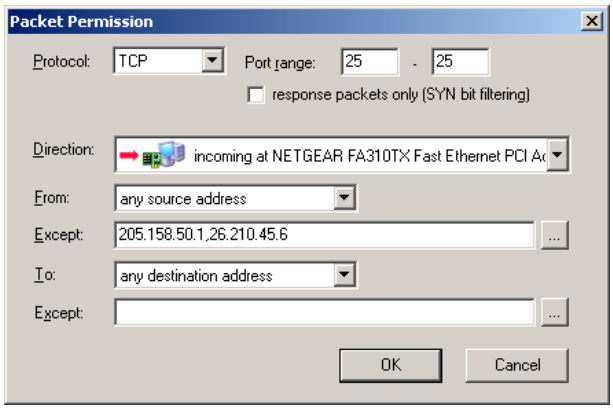
Adding new permission set
Click the **Add new permission set** radio button then click the **OK** button. Enter a **Permission set name** and click the **Add** button, the **Packet Permission** window will now appear.

Select the IP Protocol:

- **All** - All protocols of the IP protocol will be filtered
- **TCP** - Enter the port range. If you check **continuative packets only**, the firewall will drop each TCP packet with the SYN flag (the first TCP packet - TCP connection establishing packet). The firewall will not allow a TCP connection to be established for the entered ports and direction.
- **UDP** - Enter port range. Check **solicited packets** if needed.
- **ICMP** - Check those messages you want to allow. Recommended: **Outgoing Echo Request**, **Incoming Echo reply** and **Time exceeded only**.
- **Other** - The firewall can filter any IP protocol. Enter the protocol number you want to filter here.

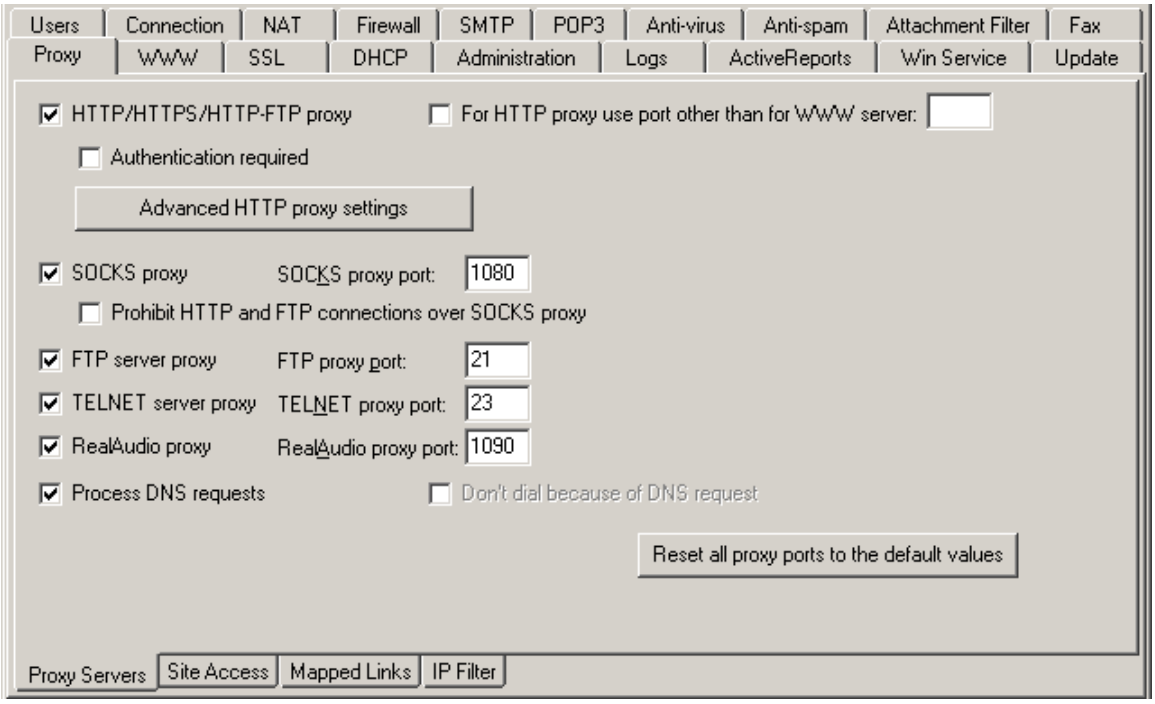
Excluding Certain IPs
Although all rules in the firewall mean ALLOW, it does have the capability to exclude addresses coming from a specific adapter. Example: Someone on the Internet is constantly connecting to your SMTP server on port 25, to fix this do the following:

1. Click the SMTP connection from the Internet to this computer rule, then click Edit set.
2. Click the TCP (port 25) rule, then click Edit.
3. For Direction, choose the interface traffic is coming from the Internet to your SMTP server (e.g. incoming at X Adapter).
4. From:/To: should be any source address.
5. The first Except: field is where you can enter the IP address(es) of the attacker. Enter addresses comma delimited in single address form (192.168.1.1) IP range form (192.168.1.1-192.168.1.20) or IP subnet form (192.168.1.0/255.255.255.0).
6. Click OK, rename the Permission set name (you can just add the number 2 to the end), click OK, then click Save. Now any address will still be able to deliver mail to your SMTP server EXCEPT the attacker(s).



Proxy

To configure secure shared Internet access through the 602LAN SUITE you must first configure the proxy and then the client's web browser. If you wish to enable user authentication for an additional amount of network control, then you will also need to setup users as described in the "Setting Up User Accounts" section of the manual.



Setting Up the Proxies

A proxy server runs on a computer that is connected to the Internet via a permanent or dial-up line. The proxy server receives requests from clients on the network and forwards them on its own. Fulfilled requests (i.e. HTML pages) are then delivered to the proper clients. The Proxy server performs two functions:

- **Proxy** – It proxies clients on the network with a connection to the Internet via the HTTP/HTTPS/HTTP-FTP application protocols.
- **Security** – Because all communication goes through the server it can check every computer that wants to communicate with any client computer on the Internet via the HTTP/HTTPS/HTTP-FTP application protocols.

The Proxy setup tab can be found by clicking on "Settings" and "Advanced Configuration" from within the 602LAN SUITE 2004 application. The Proxy tab is setup for unrestricted Internet Access by default. These settings will not need to be altered or changed for most users but can be modified depending on your individual desires or security concerns. You may activate or de-activate any or all of the 602LAN SUITE proxy services by checking or unchecking it's respective selection box. Simply altering the port number in the service's respective port field can change the port for each service. All ports are set to industry standards by default. Individual proxy services that may be activated /deactivated or have their ports modified are as follows:

- **HTTP/HTTPS/HTTP-FTP** – This is the proxy that provides Internet access via http.
- **SOCKS** – This controls the SOCKS Protocol, which is frequently used by instant messaging programs as well as programs, which do not provide direct proxy support. The SOCKS 4 and SOCKS 5 standards are supported.

© 2004 Software602, Inc. 9/2004

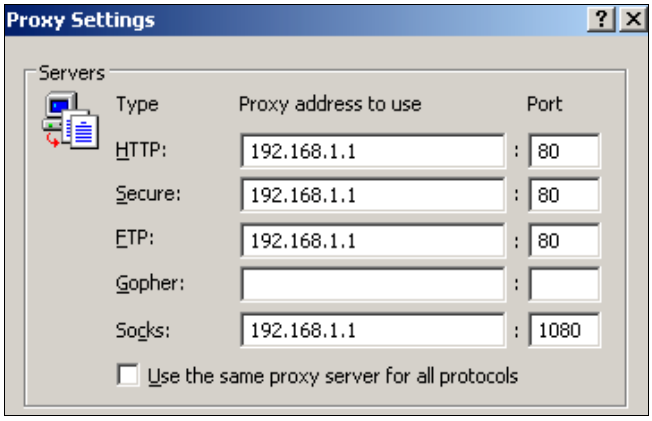
- **FTP** – This proxy controls the FTP (File Transfer Protocol), which is commonly used for the transfer of files over the Internet.
- **Telnet** – This proxy service allows the communication of telnet applications through the 602LAN SUITE application.
- **RealAudio** – This proxy is specifically designed to allow the use of the popular RealAudio program from Real Networks, Inc.
- **DNS requests** – While not a true proxy service, this option allows your 602LAN SUITE server to process DNS (Domain Name Server) requests for other PC's on the network. This is particularly useful when utilizing older applications requiring the SOCKS 4 protocol.

NOTES: To completely disable all proxy services you must uncheck all services on the proxy tab.

The HTTP/HTTPS/HTTP-FTP proxy server runs on port 80 by default. If you are running a third party web server you may need to alter this to avoid port conflicts. This will not cause a conflict when run in conjunction with 602LAN SUITE 2004's built in Web Server.

Setting Up Microsoft® Internet Explorer Web Browser

The Microsoft Internet Explorer is the preferred web browser for 602LAN SUITE 2004. You may however, use any browser type you desire. Below we have the instructions for versions 5.x and 6.x of the Internet Explorer. Please note that Automatic Proxy server detection is not supported.



Microsoft® Internet Explorer Proxy Setup

1. Open Microsoft Internet Explorer
2. Select Tools, then Internet Options
3. Click the Connection tab
4. Under the section LAN Settings, click LAN Settings.
5. Check Use a proxy server, then click Advanced.
6. Insert 192.168.1.1 (or the IP address of your 602LAN SUITE server if different)
7. For SOCKS use the port 1080 for other protocols, use their respective ports as shown in the illustration.
8. Click OK, OK again, then OK one last time

NOTES: Any application with proxy server support can be used with 602LAN SUITE's Proxy server. Please consult your applications help files for proxy configuration information and instructions.

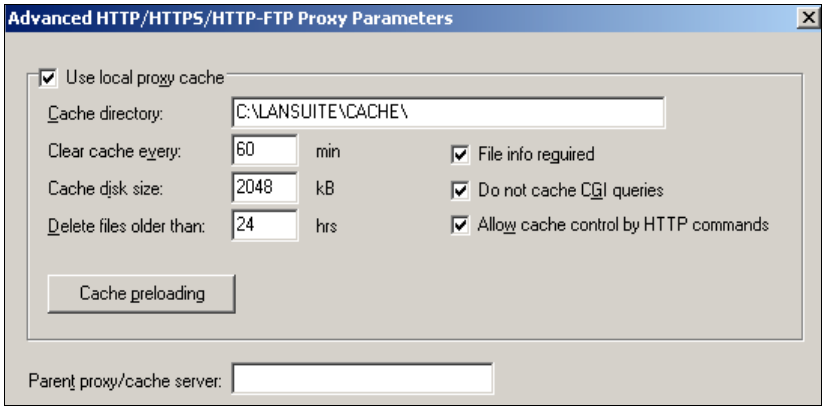
Proxy Cache

Four tabs are located on the Proxy tab. Proxy Servers - main proxy servers configuration tab and Site Access, Mapped Links, IP Filter tabs concerning security of proxy servers.

Using the Local Proxy Cache - Proxy Servers Tab

This checkbox is recommended for slow connections where bandwidth is a major concern. By selecting this checkbox, you activate the Proxy cache that stores web pages on the server allowing them to be retrieved quickly from the hard drive as opposed to slowly over a slow Internet connection. For fast connections such as DSL/Cable/T1, this feature provides little benefit. The following options are recommend to be enabled for effective cache use:

- **File info required** – Most web servers provide information on a file, this allows 602LAN SUITE to determine if the file has been downloaded completely, with this option checked, only files verified complete will be saved to the cache.
- **Do not cache CGI queries** – 602LAN SUITE will not cache results from a CGI request (dynamic web page).
- **Allow cache control by HTTP commands** – 602LAN SUITE will obey HTTP caching commands (example: Pragma: no-cache)



Cache Pre-loading

If client stations on your Local Area Network often use large files from the Internet, it is possible to preload them into the HTTP proxy cache from a storage device (i.e. CD-ROM, HD, etc.). Clients will not have to download files from the Internet site but only from the computer where 602LAN SUITE is running.

To the Preload files for URL edit line, enter the Internet site (full Internet path – URL) where requested files are originally stored. To the Preload from path edit line, enter the full path to the storage device where you have saved files for the requested URL. All pre-loaded items must be in the proper directory structure identical from the site for which they are being pre-loaded. When a client (i.e. Internet browser from your LAN) sends a request for a document on the Internet, the proxy server will first check the document on the Internet for the newest version. I you don't want let 602LAN SUITE to check it, check Do not check for new version of files at least for xx days and enter the number of days.

Parent Proxies/Third party cache servers

If your network requires that you utilize a parent proxy server, doing the following may specify this:

1. Go to the Proxy tab and click on Advanced HTTP Proxy Settings.
2. In the parent proxy/ cache server field, input the IP address of the parent proxy or cache server you wish to utilize.

Site Access Control

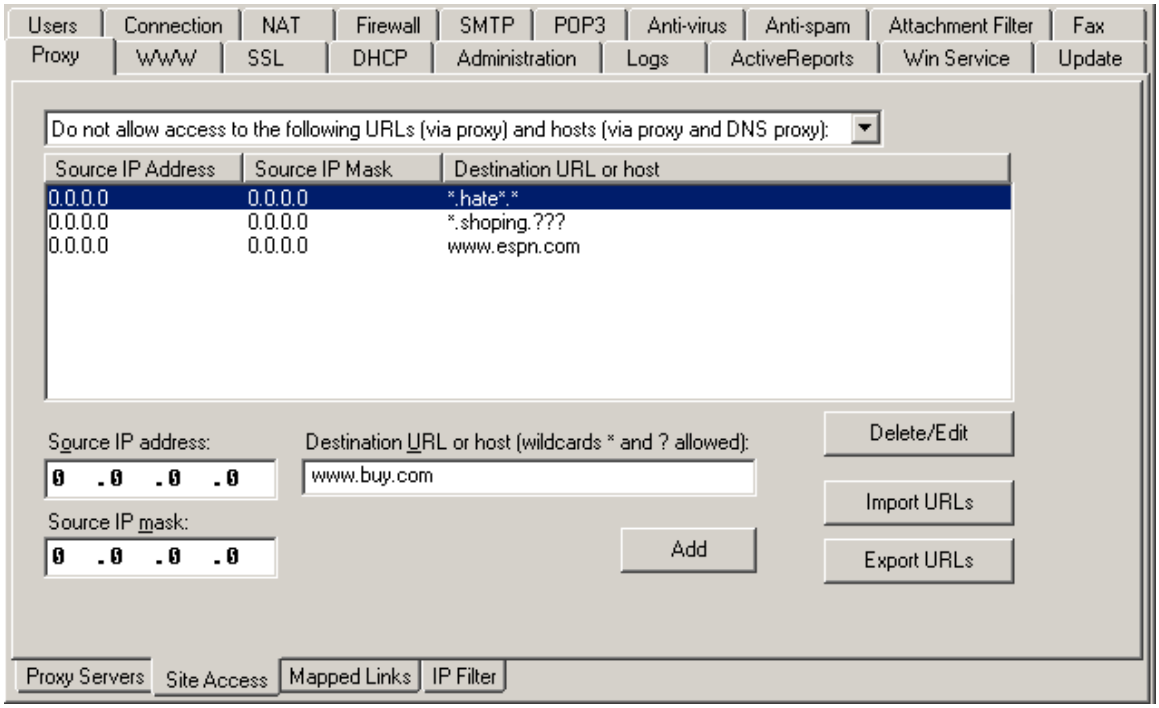
Restricted/allowed users are specified by their IP address and mask. It is possible to restrict/allow specific URLs for a single computer or sub-network. To specify the entire network input 0.0.0.0 for the Source IP and Mask. If only a specific machine or group of machines need to be denied/allowed access, put the specific IP (i.e. 192.168.1.23, mask 255.255.255.255) or group (i.e. 192.168.1.0, mask 255.255.255.0). Unlike the IP filter, the restricted/allowed sites are defined by their name or part of their name where * and ? symbols can be used (DOS convention: * = alias all, ? = mask).

Use the edit box and the Add button to enter names of restricted/allowed sites. By using * and ? characters, you can construct common masks. Enter the IP address and mask of the computer or sub-network that the URL will be restricted/allowed.

Examples to restrict access to some servers:
.hate.* restricts access to servers in which the domain name begins “hate” for all services (HTTP, HTTPS, FTP) *.shopping.??? restricts access to the domain shopping in all 3 digit endings(i.e. www.shopping.com, www.shopping.org, etc.) for all services (HTTP, HTTPS, FTP), www.espn.com restricts access to the server of the given name.

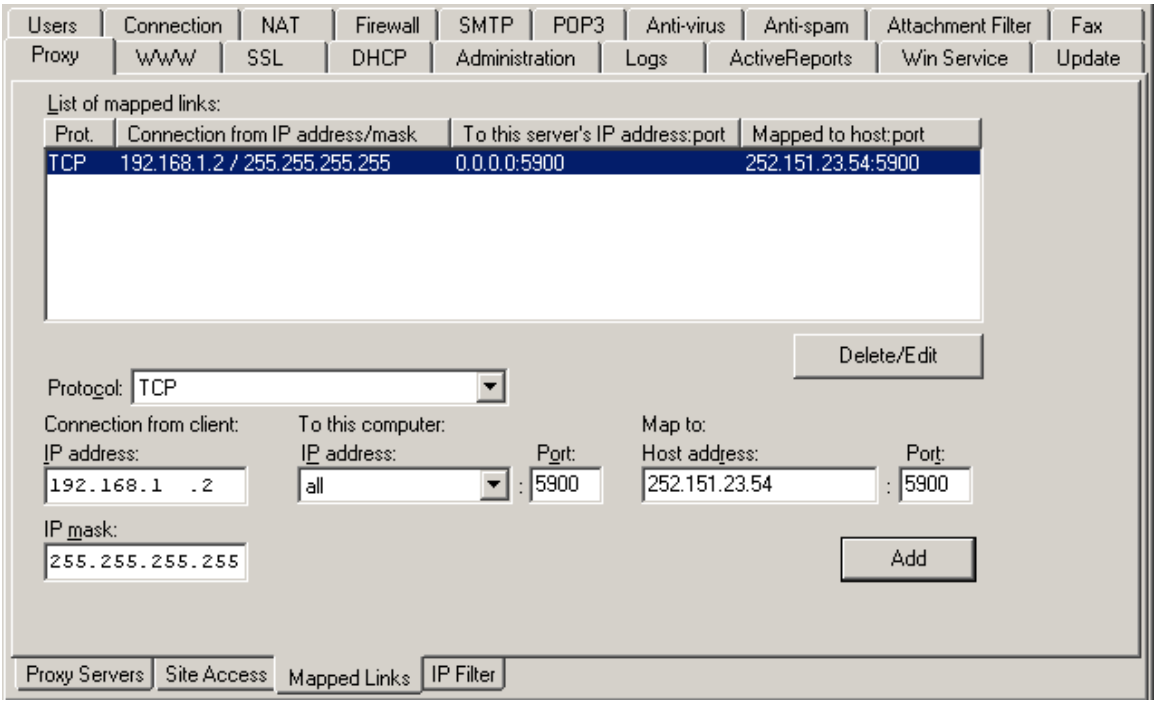
You can use the Delete/Edit button to delete or edit an already given rule.

URLs can be imported/exported from/to a file. The format of the file needs to be a plain text file with only one URL per line.



Mapped Links

Mapped Links function as an alternative for establishing a connection between a workstation connected to the LAN and a Host computer on the Internet. It is suitable for use with an application that does not supports SOCKS or PROXY and connects only with one computer on the Internet (i.e. connection to a NTTP NEWS server, VNC, POP3, etc.). It is possible to use the TCP or UDP protocol for mapped links.



Principle Function

The client program on a network workstation needs to establish a TCP/IP connection with a particular computer on the Internet. Instead of using the address of that computer, 602LAN SUITE's address is entered into the client program in which the tab Mapped Links is used to specify that if this station connects to this port, all packets should be sent to a particular computer on the Internet. This creates a virtual link between the computers through the computer where 602LAN SUITE is running. It is like a re-director that is providing a connection between two computers through the TCP/IP protocol

Advantages:

Client program does not have to contain any type of proxy/firewall support.

Disadvantages:

- Each connection requires a separate mapped link.
- Each mapped link must be setup to use a different port.

Settings

You need to setup these entries on the Mapped links tab:

- **Protcol:** Select the Protocol (TCP or UDP, UDP1, UDP2) for each mapped link. For the UDP protocol settings see below.
- **Connection from client** – The information you enter in this section is for the machines that are allowed to make the connection. Enter the IP address and IP mask of the computer that will need the mapped link.
- **IP Address:** You should enter the network address or the IP address of the machine/machines you wish to allow access to this link. Example: If you wish to allow everyone on your network and no one

else access to this link, enter your network address. If you are unsure what your network address is, you can obtain it by take taking the IP address of the 602LAN SUITE server and changing the last value to a 0 (i.e. 192.168.1.0). To let only one machine access it, enter in that machines IP Address. To allow anyone to access this link use 0.0.0.0.

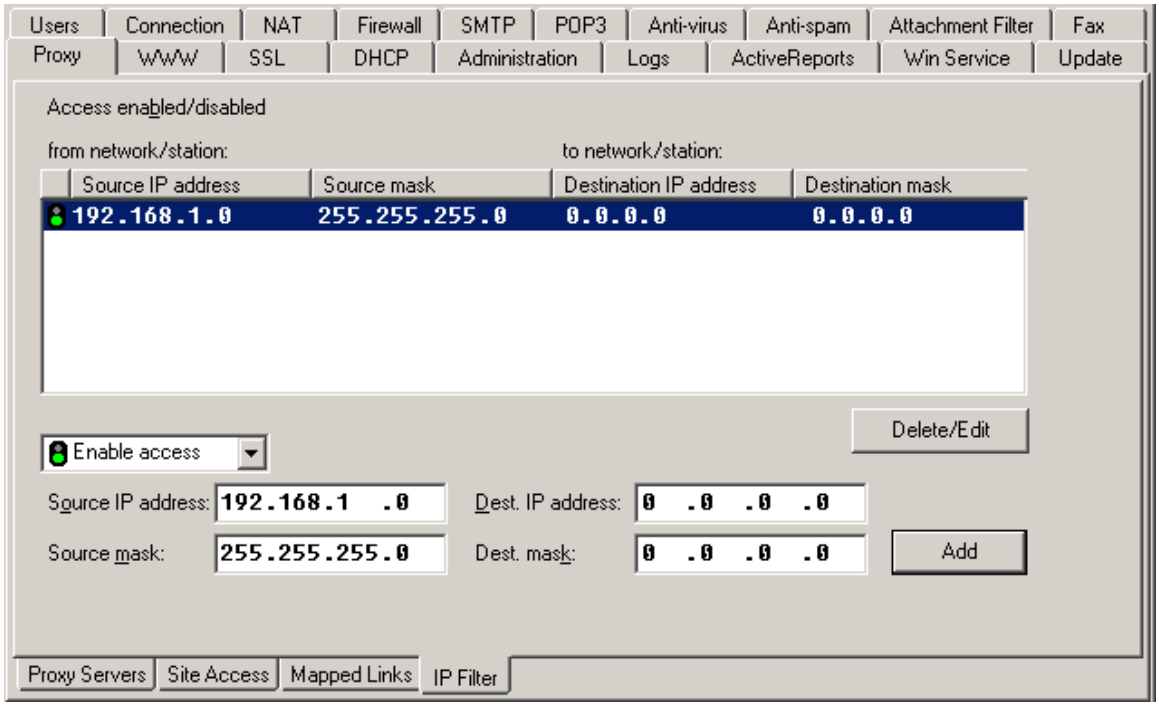
- **IP Mask:** This is the subnet mask for the machines you wish to allow. The detailed explanation of how a subnet mask works is beyond the scope of this document. The general idea of how to use it is if you only wanted one machine to access this link, it would be 255.255.255.255. If you want your entire network to access it, then enter 255.255.255.0. If you want to give everyone access, make it 0.0.0.0.
- **To this computer** – This is what interface the mapped link will be accessible from.
- **IP Address**: Set to all interfaces. The only reason this would need to be changed is if you wanted to increase security for access to the mapped link.
- **Port**: This is the port that this machine will listen on for requests coming through this link. This will vary based on what you wish to accomplish. You cannot have a port that is already in use added here. If you already have a mapped link that listens on port 9000, then you cannot add another port 9000 link. You can't use ports 80, 21, 23, and 1080 if you are using them for your proxy server. The link will not work if the port is already in use.
- **Map to:** Enter the Host address and Port. Enter the IP address and port of the host the client needs to establish a connection with.
- **Host address**: You can enter the domain name or IP address of the computer you are trying to contact. If you are trying to contact a mail server, you would enter its domain here (i.e. your ISP says that your POP3 server is pop.server.net).
- **Port**: This is the port that the computer you wish to connect to is listening on. Unlike the port under To this computer, you can reuse this port.

Be sure to click add so that the entry will appear in the window. Then click Save to save the configuration information.

WARNING: You cannot have two services using the SAME port on the SAME interface!

Proxy IP Filter Configuration

The IP filter defines what connections are possible to establish through the Proxy and SOCKS services. Through the IP filter we can define which connections can be established trough the SOCKS or Proxy Server. You will create a list of networks and stations and define if access to them is allowed or prohibited. The IP filter rules are checked from top to the bottom with each rule superceding those above it. Enter the IP address and mask of the computer or network that sends the request to the field Source IP address and Source mask. Enter an IP address and mask to the Destination IP address and Destination mask where the request is pointed. It is also necessary to define if the item is allowed or prohibited – RED means access denied, GREEN means access enabled.



Terms

A TCP/IP computer network is defined by the IP address and mask. The IP address defines the value addressed in the network and mask defines the size of the network (the maximum amount of IP addresses in a particular network).

Mask Examples

255.255.255.255 single user, the computer with IP address given above
255.255.255.0 all computers on the Class C network
255.255.255.224 subnetwork with 32 addresses
0.0.0.0 all IP addresses (all Internet)

Principle Job of the IP Filter

With the IP filter it is possible to verify whether a connection between two specific computers is allowed (i.e. a user on your network wants to connect to www.software602.com). 602LAN SUITE makes a logical decision with the IP address of the computer that wants to establish a connection (source IP address); with the IP address of the destination computer (destination IP address) and the IP Filter follows the logic operation:

To grant access, the following must apply:

SOURCE_IP AND SOURCE_MASK = WHO_IP AND SOURCE_MASK

DESTINATION_IP AND DESTINATION _MASK = WHERE_IP AND DESTINATION _MASK
The connection will be established if the result of both logic operations is true and the rule is green.
The IP filter rules are checked from top to bottom. From the red/green (disabled/enabled) rule you have two choices:

- Only grant several users Internet access.
- Only restrict several users from Internet access.

If you need to move a rule level up or down, highlight it and push Crtl + Up arrow / Crtl + Down arrow. If you want to delete any item from the list, highlight the item and press the Delete button. You can also edit the highlighted items. Their values move into the edit fields.

NOTE: If using a Parent proxy/cache server it is not possible to restrict communication using the IP mask because the Proxy Server in this case does not verify the IP address of the destination computer. For access restriction to some computers use the Site Access tab.

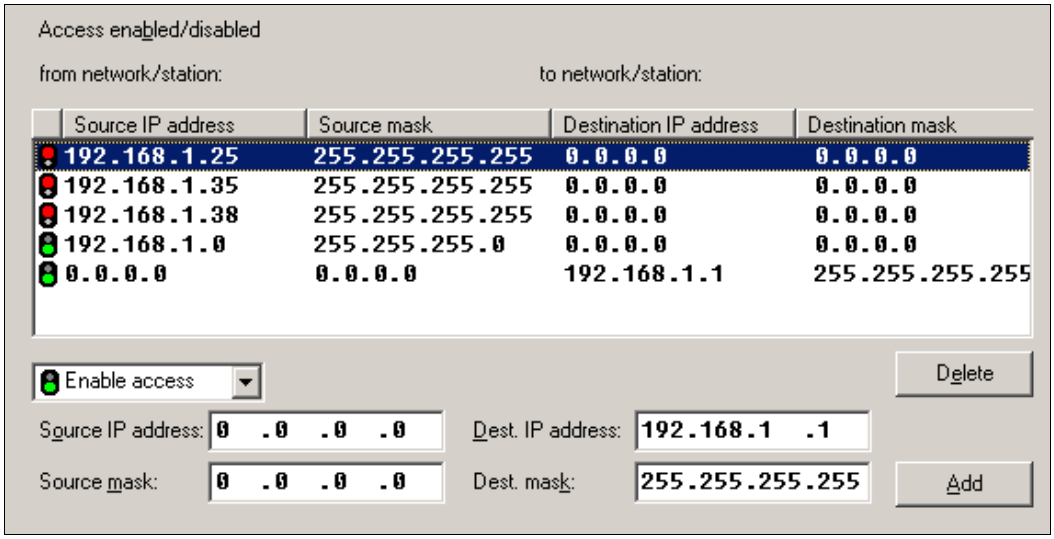
IP Filter Settings – Example 1

You need for your company the following IP filter settings:

- Restrict three employees with following IP addresses – 192.168.1.25, 192.168.1.35, 192.168.1.38
- Allow all others Internet access
- Outside users from the Internet need to have access to only one computer with the 192.168.1.1 IP address.

Solution:

- The first three rules deny the three computers 192.168.1.25, 192.168.1.35, 192.168.1.38 access to any computer through the firewall (i.e. this restricts these three employees access the Internet).
- The fourth rule grants all users of the 192.168.1.0 network communication with any computer through firewall (i.e. it allows all users including 192.168.1.25, 192.168.1.35, and 192.168.1.38 users access to the Internet). But, since the IP filter rules are checked from top to the bottom, users 192.168.1.25, 192.168.1.35, 192.168.1.38 do not have access to the Internet.
- The fifth rule grants any communication with 192.168.1.1 through the firewall (i.e. this rule allows ANY Internet users access to the 192.168.1.1 computer).

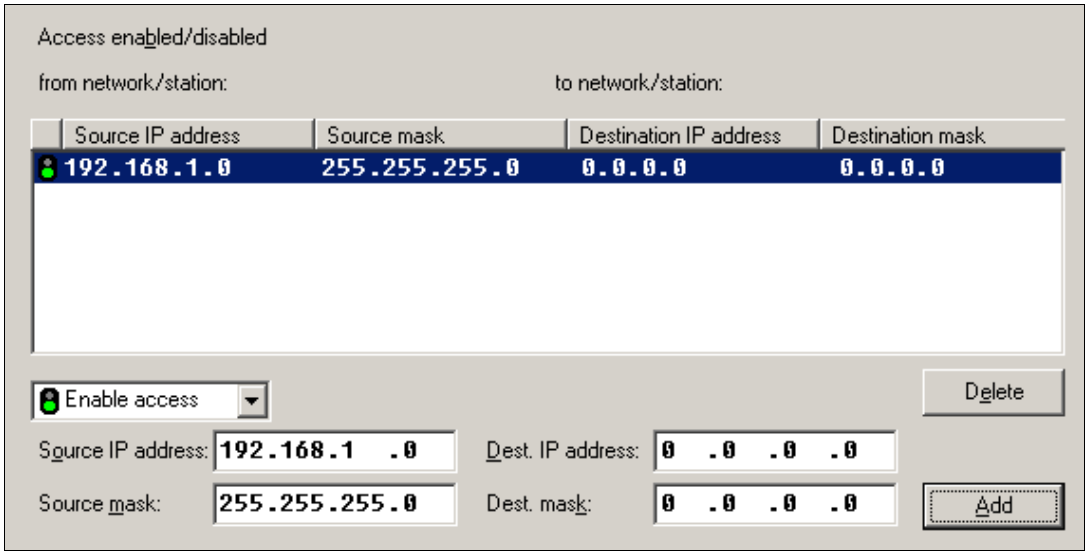


NOTE: If the fourth rule were in the first position, it would not be able to restrict those 192.168.1.25, 192.168.1.35, 192.168.1.38 users.

IP Filter Settings – Example 2
All users on the network 192.168.1.0 can communicate with any computer on the Internet and this network cannot be reached from the Internet.

Solution:

- Setup one rule that defines the internal network. The rule below states that 192.168.1.1 through 192.168.1.254 can access any destination, 0.0.0.0, which means all IP addresses.



SSL Configuration

The SSL (Secure Socket Layer) protocol runs between the network level and application level protocols. It provides server authentication, an encrypted connection and client authentication (optional). On the SSL tab you can specify SSL operation parameters and create Public & Private keys. SSL provides:

- Communication via SSL has a pair of keys: a public key and a private key.
- The Private key is used by the server to encode data.
- The Public key (certificate) is used by the client to decode the data. The certification authority (CA) usually undersigns the public key so the client can be sure that it is communicating with the correct server. The easiest configuration is by using a self-signed certificate (the server functions as a CA).

SSL provides:

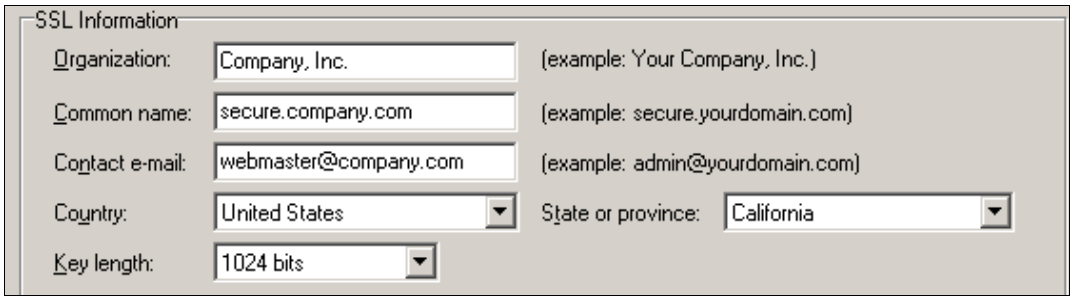
- SSL server authentication allows a user to confirm a server's identity.
- An encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software.
- SSL client authentication allows a server to confirm a user's identity.
- The handshake of the SSL protocol consists of the following steps:
- Authenticate the server to the client.
- Allow the client and server to select the cryptographic algorithms, or ciphers, that they both support.
- Authenticate the client to the server (optional).
- Use public-key encryption techniques.
- Establish an encrypted SSL connection.

The SSL tab has two sub-tabs that define values and settings for SSL used by the SSL SMTP, SSL POP3 and SSL WWW servers.

General

If you want to communicate securely between SMTP, POP3 or WWW servers and their clients, you must first create the public and private key. Enter your information for public and private key setup:

- **Organization** – Name of your organization
- **Common name** – The IP address or domain name of the computer where 602LAN SUITE is running
- **Contact e-mail** – The administrator or webmaster e-mail address
- **Country** – Select your country
- **State or province** – Select your state or province
- **Key length** – Select key length. A longer key means higher security, but more data to transmit.



Now you have the two options: create a self-signed certificate or have your public key signed by a Certification Authority (CA).

- **Sef-signed:** A self signed key is free but will not be recognized by the users web browsers and will consequently offer them a warning upon accessing the SSL server.

- **Signed by a Certification Authority (CA):** A certificate purchased from a reputable certificate Authority such as Thawte or Verisign will be widely recognized and the user's browser will automatically accept this as valid proof of security.

If your server is to be accessed only by employees or individuals that are familiar with your organization, then a self signed certificate might be the best choice for you. If you are planning on offering secure access to your server to the public, you may wish to purchase a certificate from a well know Certificate Authority to instill their confidence in your sever and its security. Both certificates are equally effective.

Create self-signed certificate

To create a self-signed certificate click the Create Self-signed Certificate button. The public key and private key are stored in a common file SERVER.PEM (in the root of your 602LAN SUITE directory). Your information (Organization name, domain name, etc.) is stored in the file SSLEAY.CFG (in the root of your 602LAN SUITE directory). If the key expires, you can always re-generate it. The file SERVER.CRT (in the root of your WWW document folder) is also generated, which enables you to add the certificate into the list of CAs.

Create Certificate Signing Request

If you want a CA to sign your public key, click the Create Certificate Signing Request (CSR) button. When the CERTIFICATE REQUEST is generated, copy it to the clipboard and insert it into a CA form on the Internet. The certificate you receive from the CA must be saved to 602LAN SUITE. Click the Input Certificate button, open the received certificate and click the Save certificate to 602LAN SUITE button.

Advanced

- **Client verification using certificates** - Used to switch on certificate verification of the client certification authority (if not checked the client only verifies the server certificate). The following two checkboxes are accessible only if this check box is active.
- **Certificate required** - After activating this checkbox, client certificate verification will be required for further communication.
- **Verify only once** - Checking this box, the WWW server will only accept certificates confirmed directly by the certification authority (and not by sub-authorities).
- **Don't use any certificates** – Certificates (self-signed or signed by a CA) will not be used for server or client authentication.
- **Server Certification File -** Holds the access path to the certificate file, which includes the public and private keys certified by the certification authority.
- **Server private key** -If the certification file does not include the private key, enter the access path to the file that includes this key into the field Server private key (if encrypted in a separate file).
- **CA files directory** - Enter the access path to the directory with files including the public keys of each certificate authority into the field CA files directory.
- **CA database file** - Files with public keys can also be merged into a single file called a CA database file. This can be done by copying all individual certificates into a single file.
- **Just talk SSLv2** – 602LAN SUITE will communicate with clients by SSL version 2 only.
- **Just talk SSLv3** – 602LAN SUITE will communicate with clients by SSL version 3 only.
- **Do not generate a temporary RSA key** – No temporary RSA key for default SSL authentication will be generated.
- **Turn on SSL bug compatibility** – Some older browsers contain an SSL bug. If you have problems with SSL connections using an older browser, check the Turn on SSL bug compatibility checkbox.

You can use various encoding methods for communication among SSL servers and their clients. Use the range of checkbox Ciphers to specify the methods that will be accepted by the SSL server.

Appendix

Hayes Compatible Modem Commands

Here is a complete list of the Hayes compatible command set. Not all modems/ faxmodems use the whole list of commands and some of them use special commands. This information is provided for advanced users (dial-up connection or fax settings).

Almost all commands begin with AT (attention) letters. In some cases capital letters are required.

AT Attention – begins all commands except '+ + +', '/A', 'A>'
ATA Picks up the phone and tries to establish a connection to the incoming call
ATB Switches between the BELL and CCITT standard.
A/ Repeats the previous command.
A> Repeats the previous command until any key is pressed
ATC Enables transmission:
ATC0 transmission prohibited
ATC1 transmission enabled (default)

ATD dialing number (character "," = delay 2 sec.) The following characters can be placed after ATD:

- **T** tone dialing mode
- **P** pulse dialing mode
- **R** automatic answer mode (picks up the phone immediately after ringing)
- **W** it waits for dialtone before dialing out
- **,** delay before next dial attempt (about 2 sec. – according to S8 register setting)
- **@** delay according to S7 register setting
- **!** hangup phone for 0.5 sec then continues
- **;** switch to command mode (as last character)
- **S** dials the number saved in the modem

ATE Command echo:
ATE0 enabled – display pressed keys
ATE1 disabled
ATF Switching between half duplex and full duplex:
ATF1 modem displays transmitted data
ATF2 modem does not display transmitted data
ATH Hang up command:
ATH0 hang up
ATH1 pick up
ATI Displays modem information.
ATL Sets loudspeaker volume:
ATL0 very low
ATL1 low
ATL2 middle
ATL3 high
ATM Loudspeaker operation:
ATM0 on
ATM1 on when a connection is established
ATM2 constantly turned on
ATM3 turned off when dialing out and receiving a signal
ATO Switching to transmission data mode:
ATO0 switching from command mode to transmission mode
ATO1 special according to device
ATQ Display answers to commands:
ATQ0 enabled

ATQ1 disabled
ATS Modem internal registers setting:
ATSr=n setting S-register to number r
ATSr? checking S-register for number r
ATV Switching between numeric and character answer to command:
ATV0 numeric answer 'AT'-(0)
ATV1 character answer 'AT'-'OK'.
AT&W Save modem configuration into its internal memory
ATX Hayes Smartmodem 300 compatible result codes (i.e. BUSY, CONNECT 9600, etc.)
ATZ Modem reset
AT&Z Saves telephone number (if possible). You can call this saved number by ATDS command
+ + + Switch from transmission to command mode

E-mail Settings Example

A company is connected to the Internet via a dial-up. The company has purchased a domain, company.com, and the Internet Provider has setup a single POP3 account that will contain all e-mail for that domain. Employees use MS Outlook Express as an e-mail client.

Solution

Collecting the Common Domain Box

Each user will have a box created on the 602LAN SUITE server. It is recommended to use names that are part of the e-mail address (i.e. bob@company.com should have the name bob). Otherwise it would be necessary to enter these names or complete addresses as the user's alias address. On the Users tab for the Default domain type the domain (in this case, company.com). On the POP3 tab, enter the mailbox obtained from your Internet Provider that contains all the e-mail for the domain, company.com and For 602Pro user select according to the address. Outlook Express users will enter their e-mail addresses in the form of name@company.com. This ensures that replies to messages will be received correctly to the Internet POP3 mailbox. Users will enter the IP address of the computer on which 602LAN SUITE runs as the POP3 server and SMTP server address.

Message Receiving

The 602LAN SUITE server will dial a connection to the Internet and transfer messages from POP3 mailboxes (specified on the POP3 tab) into internal POP3 mailboxes. Once this is done, each user will be able to collect their mailbox on the 602LAN SUITE server.

Message Sending

Users will create their messages and Outlook Express will send these to the 602LAN SUITE server. The server will execute the relay function, dial the connection to the Internet and send the messages (without any change in addresses) according to the settings on the SMTP.

Troubleshooting Common Error Messages

- **We do not relay** - The e-mail you are attempting to send through 602LAN SUITE is not in compliance with your relay settings. The most common cause of this is that the e-mail address domain does not match the Default Domain or the user's aliases in the Users tab.
- **DNS: Host not found** - This occurs when you attempt to send mail to a domain that does not exist. Check the e-mail address and try again.
- **Unable to locate MX records for domain** - You will need to add the DNS entries for your Internet connection in the DNS1 and DNS2 fields in the Advanced Sending Parameters on the SMTP tab in your Advanced Configuration. If you do not know what the DNS server's IP addresses are, please contact your ISP.
- **Your IP address has changed from your last access to the 602LAN SUITE Webmail. Please login again** - This error indicates that the IP address assigned by your ISP to your connection has changed. Typically, this happens on large ISPs such as AOL that use proxy servers to fetch web pages rather than provide a direct client connection. You will need to use another ISP to check your web mail remotely.
- **Server Certificate File is not defined** - This error indicates that the SSL WWW server has been activated but no SSL certificate has been defined. You can create a self signed certificate from the SSL tab in the Advanced Configuration.
- **Error: Cannot initialize AVG kernel** - This error indicates that the AVG anti-virus program has not been installed on the server or can not load. Typically reinstalling AVG will correct this problem.
- **"Transmission Interrupted" error message when sending a fax** - This error is attributed to three things: Line noise, an incorrect Windows modem profile, or a bad modem initialization string. Your local telephone company can sweep your telephone lines to clear up any line noise, and your modem manufacturer should be able to provide you with the proper modem driver/profile and an optimized modem string. Note that 602LAN SUITE does not support CAPI modems or virtual TAPI modems that are often created by ISDN or CAPI modems.
- **SendFax client: Unable to run program for sending fax** - This is because the SendFax client cannot communicate with the 602LAN SUITE server. This is usually caused by the SMTP server being disabled, a port conflict on port 25 caused by another SMTP server already using the port, or the IP address of the 602LAN SUITE server has changed. The SMTP server can be enabled by checking the SMTP server checkbox on the SMTP tab under Advanced Configuration. Try to "ping" the server from the workstation. See the "Unable to initialize SMTP server" topic for information about troubleshooting port conflicts.
- **Unable to initialize SMTP server (Port already in use?)** - This error occurs when 602LAN SUITE can not open the SMTP port (port 25 by default). This is usually caused by another program that is attempting to use the SMTP port. Common programs known to cause this problem are the SMTP service that is installed with Internet Information Services (IIS), Norton Antivirus, and many different viruses and trojan horses with built-in SMTP mail servers (Sircam, Iloveyou, etc.).

© 2004 Software602, Inc. 9/2004

A

Access Filter, 19
ActiveReports, 3, 5, 52, 53, 54
Adding a new set, 58
Address Book, 3, 5, 31, 37, 38, 39, 40, 41, 49
Aliases, 11, 21, 36
Anti-spam, 3, 5, 41, 45, 46, 47, 48
Anti-virus, 3, 5, 6, 16, 41
APOP, 14
ATRN, 13, 14
AVG, 16, 73

B

Bayesian, 5, 45, 46, 47, 48
BitDefender, 5, 16
Blacklist, 5, 43, 45, 46, 48
Blind copies, 39

C

Cache Pre-loading, 61
Certification, 16, 68, 69
Ciphers, 69
CSR, 69
Custom Security Level, 57

D

Default Domain, 9, 73
DHCP option, 34
DHCP server, 3, 34
Dial-up, 7, 8, 31, 45, 51
Dial-up Connection, 7
Dial-up schedule, 7
Directory Browsing, 19
DNS proxy, 34
DNS requests, 60
DNS-bl, 45
DNSBL, 45

E

EHLO, 35
Environment variables, 18, 21
ETRN, 13, 14
Export, 11, 39

F

FastCGI, 3, 18, 20, 21
Fax ID, 4
Fax Identification, 22
Fax server, 3, 4, 31
Firewall, 3, 4, 6, 32, 55, 56, 57, 58, 63, 66
Firewall messages, 32
FTP, 3, 4, 10, 18, 19, 20, 29, 30, 56, 60, 62

G

Grisoft, 16

H

HELO, 35
Home directory, 4, 18
HTTP/HTTPS, 3, 4, 10, 59, 60

I

Import, 11, 39, 43
Internet Explorer, 6, 20, 30, 60
IP Filter, 3, 4, 29, 30, 36, 61, 65, 66, 67

J

Junk, 38, 43, 45, 46, 47, 48

K

Key length, 68

L

LDAP, 3, 4, 5, 11, 31, 40, 49, 55, 57
Logs, 31

M

Mailbox Size Limit, 11
Mapped Applications, 21
Mapped Links, 61, 63
Message Header, 41
Modem Commands, 23, 70

N

NAT, 3, 4, 6, 26, 34
Not Junk, 38, 43, 45, 46, 47
NT Service, 33

O

ONCONN.BAT, 8
Outlook Express, 3, 5, 17, 36, 40, 49, 72

P

Permanent, 7, 8
POP3 Server, 3, 14
Proxy, 4, 8, 9, 10, 26, 31, 55, 59, 60, 61, 65, 66
Proxy Cache, 61
Proxy IP Filter, 65

© 2004 Software602, Inc. 9/2004

R

RealAudio, 3, 4, 10, 60
Remote administration, 29, 30
Rules, 41

S

Script directory, 18
Security, 12, 14, 57, 59
SendFax Client, 24
Site Access, 61, 62, 66
SMTP relay, 36
SMTP Server, 3, 12, 13, 36, 45
SOCKS, 3, 4, 8, 10, 31, 52, 59, 60, 63, 65
Speed Limit, 24
Spell Check, 39
SSL certificate, 12, 14, 20, 73
SSL POP3, 3, 14, 57, 68
SSL SMTP, 3, 12, 68

T

TAPI, 3, 4, 8, 22, 23, 25, 73
Telnet, 3, 4, 10, 60
Text Signature, 39
Troubleshooting, 73

U

User Folders, 19
User Name, 9, 11, 14, 17

V

VPN, 7, 8

W

W3C, 31
WAP, 37, 44
Web Based Administration, 28, 29
Web Mail, 3, 11, 17, 20, 37, 40, 43, 45, 47, 48, 73
Web Server, 18, 19, 20, 60
Whitelist, 5, 43, 45, 46, 47, 48
Windows Service, 28, 29, 33
WWW server, 17, 18, 19, 20, 21, 29, 30, 31, 68, 69, 73

© 2004 Software602, Inc. 9/2004